PROFESSIONAL MASTER'S THESIS

A STRUCTURED METHODOLOGY FOR THE DIRECTION AND PLANNING PHASE OF THE CYBER THREAT INTELLIGENCE CYCLE: REDUCING INFORMATIONAL NOISE AND ALIGNING WITH THE REGULATORY FRAMEWORK OF THE BRAZILIAN NATIONAL FINANCIAL SYSTEM

Pedro Henrique Silva Gontijo

Brasilia, January of 2026

UNIVERSITY OF BRASILIA

Faculty of Technology
DEPARTMENT OF ELECTRICAL ENGINEERING

UNIVERSITY OF BRASILIA
Faculty of Technology

PROFESSIONAL MASTER'S THESIS

A STRUCTURED METHODOLOGY FOR THE DIRECTION AND PLANNING PHASE OF THE CYBER THREAT INTELLIGENCE CYCLE: REDUCING INFORMATIONAL NOISE AND ALIGNING WITH THE REGULATORY FRAMEWORK OF THE BRAZILIAN NATIONAL FINANCIAL SYSTEM

Pedro Henrique Silva Gontijo

Professional Master's Thesis submitted to the Department of Electrical Engineering as a partial requirement to obtain the degree of Master in Electrical Engineering

Examination Board

Prof. João José Costa Gondim, Ph.D, FT/UnB ______________________
Advisor

Prof. Laerte Peotta de Melo, Ph.D, FT/UnB ______________________
Internal Examiner

Prof. Dino Macedo Amaral, Ph.D, Banco do Brasil ______________________
External Examiner

Prof. Fábio Lúcio L. de Mendonça, Ph.D, FT/UnB ______________________
Alternate Examiner

CATALOG SHEET

GONTIJO, PEDRO H. S.
A STRUCTURED METHODOLOGY FOR THE DIRECTION AND PLANNING PHASE OF THE CYBER THREAT INTELLIGENCE CYCLE: REDUCING INFORMATIONAL NOISE AND ALIGNING WITH THE REGULATORY FRAMEWORK OF THE BRAZILIAN NATIONAL FINANCIAL SYSTEM [Federal District] 2026.
xvi, 51 p., 210 x 297 mm (ENE/FT/UnB, Master, Electrical engineering, 2026).
Professional Master's Thesis - University of Brasilia, Faculty of Technology.
Department of Electrical Engineering
1. Cyber Threat Intelligence 2. Direction and Planning
3. Priority Intelligence Requirements 4. Brazilian Financial System
I. ENE/FT/UnB II. Title (Series)
PUBLICATION: PPEE.MP.108

BIBLIOGRAPHIC REFERENCE

GONTIJO, P. H. S. (2026). *A STRUCTURED METHODOLOGY FOR THE DIRECTION AND PLANNING PHASE OF THE CYBER THREAT INTELLIGENCE CYCLE: REDUCING INFORMATIONAL NOISE AND ALIGNING WITH THE REGULATORY FRAMEWORK OF THE BRAZILIAN NATIONAL FINANCIAL SYSTEM* . Professional Master's Thesis, Department of Electrical Engineering, University of Brasilia, Brasilia, DF, 51 p.

ASSIGNMENT OF RIGHTS

AUTHOR: Pedro Henrique Silva Gontijo
TITLE: A STRUCTURED METHODOLOGY FOR THE DIRECTION AND PLANNING PHASE OF THE CYBER THREAT INTELLIGENCE CYCLE: REDUCING INFORMATIONAL NOISE AND ALIGNING WITH THE REGULATORY FRAMEWORK OF THE BRAZILIAN NATIONAL FINANCIAL SYSTEM .
GRADE: Master in Electrical Engineering YEAR: 2026

Dept. of Electrical Engineering (ENE) - FT
University of Brasilia (UnB)
Darcy Ribeiro Campus
CEP 70919-970 - Brasilia - DF - Brazil

DEDICATION

To my mother, who always guided us along the path of education, remaining present at every stage of our lives. This work is a reflection of her dedication, strength, and the countless efforts she invested in me and my sister, to whom I am also deeply grateful.

To my wife, who has supported this journey since its earliest stages, with patience, partnership, and unwavering presence. Her strength and dedication, especially while caring for our daughter during many demanding moments—including this very moment as I write these words—made this work possible.

To my daughter, who inspires me every day with her intelligence, curiosity, and love of learning. Her preference for books over toys, even at such a young age, continually reminds me of the true value of knowledge.

And to my son, who is yet to be born, but already inspires me to build a better future.

ACKNOWLEDGEMENTS

First and foremost, I thank God, whose grace, strength, and guidance have sustained me throughout this journey.

I would like to express my deepest gratitude to my advisor, Prof. Ph.D. João José Costa Gondim, for his invaluable guidance, academic rigor, and constant encouragement. His mentorship played a central role in shaping the direction and depth of this research.

I am also sincerely thankful to my co-advisor, Prof. Ph.D. Robson de Oliveira Albuquerque, for his insightful feedback, technical expertise, and steady support at every critical stage of this work.

To my family and friends—thank you for being a constant source of strength, patience, and motivation. Your belief in me, especially during the most challenging moments, made all the difference.

A special acknowledgment is extended to the Military Police of the Federal District, where I served for nearly fifteen years. In particular, I am grateful for the formative experience gained within the Special Operations Battalion (BOPE – Batalhão de Operações Especiais), where I served as a Sergeant in both Intelligence functions and Tactical Operations Teams. The principles inherent to Special Operations have profoundly shaped my professional mindset.

This work is not mine alone—it is the result of many hands, voices, and silent prayers. I am grateful for each one.

ABSTRACT

The exponential growth of cyber threats targeting Critical Infrastructures has intensified the problem of information overload within Cyber Threat Intelligence (CTI) operations. Although CTI is widely adopted as a proactive cybersecurity capability, its effectiveness is frequently constrained by indiscriminate data collection practices that overwhelm analysts and weaken strategic relevance. This challenge is particularly critical in the Brazilian National Financial System (SFN), where recent prescriptive regulatory updates have transitioned CTI from a recommended capability to a mandatory technical control, requiring institutions to monitor the surface, deep, and dark web with absolute traceability. This dissertation proposes a structured methodology for the Direction and Planning phase of the intelligence cycle, aimed at reducing informational noise and aligning intelligence production with regulatory and operational requirements. The methodology is grounded in classical intelligence doctrine and organized into five stages: Strategic Alignment of critical assets, Threat Mapping, definition of Priority Intelligence Requirements (PIRs), formulation of Requests for Information (RFIs), and development of an audit-oriented Collection Plan based on the 5W3H framework. The proposed approach was implemented through an automation layer integrated into the OpenCTI platform, translating governance-level intelligence requirements into deterministic filtering rules. A conceptual case study using real open-source threat intelligence feeds demonstrated a noise reduction of 99.58%, reducing an initial dataset of 216,208 STIX Domain Objects to 903 SFN high-fidelity intelligence artifacts. The results confirm that the strategic alignment of intelligence requirements with institutional needs and the prescriptive regulatory landscape significantly enhances relevance, ensuring auditable compliance and shifting CTI operations from the exhaustive triage of ephemeral Indicators toward behavior-focused, decision-oriented intelligence.

Keywords: Cyber Threat Intelligence; Direction and Planning; Priority Intelligence Requirements; OpenCTI; Brazilian Financial System.

RESUMO

Metodologia Estruturada para a Fase de Direção e Planejamento do Ciclo de Inteligência de Ameaças Cibernéticas: Redução de Ruído Informacional e Alinhamento às Exigências Regulatórias do Sistema Financeiro Nacional

O crescimento exponencial das ameaças cibernéticas direcionadas a Infraestruturas Críticas intensificou o problema da sobrecarga informacional nas operações de Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence – CTI). Embora a CTI seja amplamente adotada como uma capacidade proativa de cibersegurança, sua efetividade é frequentemente limitada por práticas indiscriminadas de coleta de dados, que sobrecarregam os analistas e enfraquecem a relevância estratégica das informações produzidas. Esse desafio é particularmente crítico no Sistema Financeiro Nacional (SFN), onde os arcabouços regulatórios exigem que as atividades de cibersegurança estejam explicitamente alinhadas aos perfis de risco institucionais e sustentadas por mecanismos de governança auditáveis. Esta dissertação propõe uma metodologia estruturada para a fase de Direção e Planejamento do Ciclo de Inteligência, com o objetivo de reduzir o ruído informacional e alinhar a produção de inteligência aos requisitos regulatórios e operacionais. A metodologia é fundamentada na doutrina clássica de inteligência e organizada em cinco etapas: Alinhamento Estratégico dos ativos críticos, Mapeamento de Ameaças, definição de Requisitos Prioritários de Inteligência (Priority Intelligence Requirements – PIRs), formulação de Requisições de Informação (Requests for Information – RFIs) e desenvolvimento de um Plano de Coleta baseado no framework 5W3H. A abordagem proposta foi implementada por meio de uma camada de automação integrada à plataforma OpenCTI, traduzindo requisitos de inteligência em nível de governança em regras determinísticas de filtragem. Um estudo de caso conceitual, utilizando fontes reais de inteligência de ameaças de código aberto, demonstrou uma redução de ruído de 99,58%, reduzindo um conjunto inicial de 216.208 objetos para 903 artefatos de inteligência de alta relevância para o SFN. Os resultados comprovam que a harmonização dos requisitos de inteligência com as necessidades institucionais e o arcabouço normativo vigente eleva a relevância das informações produzidas, garante a conformidade auditável e redireciona as operações de CTI da triagem exaustiva de Indicadores técnicos efêmeros para uma inteligência estratégica focada em comportamentos adversários e na tomada de decisão.

Palavras-chave: Inteligência de Ameaças Cibernéticas; Direção e Planejamento; Requisitos Prioritários de Inteligência; OpenCTI; Sistema Financeiro Nacional.

INDEX

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS

Acronyms

API	Application Programming Interface
BCB	*Banco Central do Brasil*
CBEST	Cyber Best (Threat Intelligence-Led Assessments)
CI / CIs	Critical Infrastructure / Critical Infrastructures
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMN	*Conselho Monetário Nacional*
CNCiber	National Cybersecurity Committee
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CTI-CMM	Cyber Threat Intelligence Capability Maturity Model
DDoS	Distributed Denial of Service
DORA	Digital Operational Resilience Act
DP	Direction and Planning
EGNN	Edge Propagation Graph Neural Network
ENSIC	National Strategy for Critical Infrastructure Security
ETIP	Enriched Threat Intelligence Platform
FS-ISAC	Financial Services Information Sharing and Analysis Center
GF	Global-Finance
HTTPS	Hypertext Transfer Protocol Secure
HUMINT	Human Intelligence
IoC / IoCs	Indicator of Compromise / Indicators of Compromise
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
JSON	JavaScript Object Notation
LLM / LLMs	Large Language Model / Large Language Models
MITRE ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
MTTT	Mean Time to Triage
NLP	Natural Language Processing
NRR	Noise Reduction Rate
OSINT	Open Source Intelligence
OTX	Open Threat Exchange
PIR / PIRs	Priority Intelligence Requirement / Priority Intelligence Requirements
PLANSIC	National Plan for Critical Infrastructure Security
PNCiber	National Cybersecurity Policy

PSTI	Payment Service Technology Provider
RCTI	Requirement-Cyber Threat Intelligence
RCE	Remote Code Execution
RFI / RFIs	Request for Information / Requests for Information
RSFN	SFN Network
SCO / SCOs	STIX Cyber-observable Object / STIX Cyber-observable Objects
SDO / SDOs	STIX Domain Object / STIX Domain Objects
SFN	Brazilian National Financial System (*Sistema Financeiro Nacional*)
SIGINT	Signals Intelligence
SIR / SIRs	Specific Information Requirement / Specific Information Requirements
SOC	Security Operations Center
SPI	Instant Payment System
SRO / SROs	STIX Relationship Object / STIX Relationship Objects
STIX	Structured Threat Information Expression
STR	Reserve Transfer System
TAXII	Trusted Automated Exchange of Intelligence Information
TIBER-EU	Threat Intelligence-based Ethical Red Teaming for the EU
TIP	Threat Intelligence Platform
TLPT	Threat-Led Penetration Testing
TTP / TTPs	Tactics, Techniques, and Procedures
URL	Uniform Resource Locator

1 INTRODUCTION

This chapter establishes the context for the research, highlighting the critical role of the Brazilian National Financial System (SFN) within the national cybersecurity landscape. It articulates the central research problem and defines the objectives aimed at resolving this issue through a structured Direction and Planning methodology. Furthermore, it presents the justification for the study, emphasizing the strategic necessity of aligning technical Cyber Threat Intelligence (CTI) operations with the governance and risk management mandates, especially in light of the prescriptive regulatory updates of 2025.

1.1 CONTEXTUALIZATION AND MOTIVATION

The accelerated digital transformation of contemporary societies has significantly increased the interconnection, automation, and interdependence of critical systems. While this transformation enables efficiency and scalability, it also expands the cyber threat surface, resulting in an environment where cyber threats are increasingly frequent, sophisticated, and capable of producing systemic impacts. In this context, Critical Infrastructures (CIs) are defined as assets, services, systems, or networks whose disruption, degradation, or destruction may cause severe consequences to national security, economic stability, or public safety (4, 5).

Among the various sectors classified as critical, the financial sector stands out due to its central role in economic stability and its high level of digitalization. The Brazilian National Financial System concentrates essential services such as payments, credit operations, capital markets, and financial intermediation, making it a strategic target for cybercriminal groups and state-sponsored threat actors (6). Attacks against this sector may propagate cascading effects across other critical domains, amplifying their societal and economic impact.

In response to this evolving threat landscape, organizations have increasingly adopted Cyber Threat Intelligence as a proactive capability to support cybersecurity decision-making. CTI encompasses the systematic planning, collection, analysis, and dissemination of information related to adversaries capabilities, intentions, and operational behaviors, with the objective of anticipating threats and reducing organizational exposure to cyber risks (7). This intelligence-driven approach represents a shift from reactive security models toward anticipatory and risk-informed defense strategies.

Within the Brazilian context, the protection of the SFN is not only an operational concern but also a matter of state sovereignty. The National Strategy for Critical Infrastructure Security (ENSIC), established by Decree No. 10.569/2020, explicitly identifies the financial sector as a priority domain requiring enhanced protection to ensure service continuity (8). Complementarily, the National Cybersecurity Policy (PNCiber), instituted by Decree No. 11.856/2023, reinforces the need for resilience, risk management, and coordinated information sharing among public and private organizations (5).

At the regulatory level, the framework was significantly strengthened in December 2025. While Resolution BCB No. 85/2021 (9) and Resolution CMN No. 4.893/2021 (10) initially mandated cybersecurity policies aligned with risk profiles, the subsequent Resolution CMN No. 5.274/2025 and Resolution BCB No. 538/2025 introduced more prescriptive requirements (11, 12). These new standards explicitly demand "cyber intelligence actions", including the active monitoring of threats across the open internet, Deep Web, Dark Web, and private communication groups (13). These requirements transition CTI from a recommended capability to a mandatory, auditable technical control.

Despite the growing adoption of CTI and its increased regulatory weight, its operational effectiveness remains constrained by a critical challenge: the excessive volume of threat data generated by heterogeneous intelligence sources. The widespread use of Open Source Intelligence (OSINT) feeds and automated ingestion mechanisms often results in large volumes of unstructured and low-relevance data, which may overwhelm analysts rather than support decision-making (7, 14). Consequently, financial institutions face difficulties in transforming raw threat data into actionable intelligence that is both context-aware and compliant with the heightened technical expectations established by recent regulations.

1.2 RESEARCH PROBLEM

The central problem addressed in this research is the absence of structured, operational, and replicable methodologies for the Direction and Planning (DP) phase of the Cyber Threat Intelligence cycle, particularly within the context of the SFN.

According to the UK Government's "Threat Intelligence: A Guide for Decision Makers and Analysts" (2), effective CTI programs should follow the classical Intelligence Cycle, a foundational model rooted in military and governmental intelligence doctrine. This cycle comprises four interdependent phases: Direction and Planning, Collection, Analysis, and Dissemination (2, 15, 16, 17, 18, 19). The Direction and Planning phase is responsible for translating strategic objectives and decision-makers needs into prioritized intelligence requirements, thereby governing the relevance and efficiency of all subsequent phases.

Academic literature and practitioner-oriented frameworks, such as the CTI Capability Maturity Model (CTI-CMM), consistently emphasize that the Direction and Planning phase is the most critical element of the intelligence cycle, as it ensures alignment between intelligence production, organizational risks, and decision-making processes (20, 21). However, in real-world CTI operations, this phase is frequently underdeveloped, informally executed, or entirely neglected (14).

The cybersecurity industry has predominantly focused on downstream technical capabilities, including the deployment of Threat Intelligence Platforms (TIPs), the ingestion of Indicators of Compromise (IoCs), and the automation of enrichment processes. While these capabilities are essential, the lack of structured upstream planning often leads to indiscriminate data collection, resulting in informational overload and misalignment with institutional priorities (7).

This challenge is particularly pronounced within the SFN, where the updated regulatory framework explicitly requires cybersecurity practices to be compatible with each institution's risk profile and demands detailed traceability of operations (11, 12). In this environment, intelligence must be demonstrably relevant, traceable to business risks, and auditable from a governance perspective, satisfying the 14 procedures and controls now required by the Central Bank.

Therefore, the research gap lies in the lack of methodologies that systematically integrate strategic governance elements—such as critical asset identification and risk assessment—with the technical operationalization of CTI, including automated filtering mechanisms embedded within Threat Intelligence Platforms. Based on this gap, the research problem is formulated as follows:

> *How can a structured Direction and Planning methodology be operationalized and empirically evaluated to demonstrate measurable reductions in informational noise and improvements in actionable intelligence, while ensuring alignment with the regulatory requirements of the Brazilian National Financial System?*

1.3 OBJECTIVES

This section defines the general and specific objectives that guide the development and validation of the proposed Direction and Planning methodology. The objectives translate the research problem into concrete and measurable steps, ensuring a structured progression from the conceptual definition of intelligence requirements to their operational implementation within a Threat Intelligence Platform and subsequent empirical evaluation.

1.3.1 General Objective

To develop and validate a structured methodology for the Direction and Planning phase of the CTI cycle, aimed at reducing informational noise and aligning intelligence production with the operational and regulatory requirements of the SFN, using the OpenCTI platform as a reference implementation.

1.3.2 Specific Objectives

To achieve the general objective, the following specific objectives were defined:

1. **Define a Taxonomy of Intelligence Requirements:** Establish a structured framework for Priority Intelligence Requirements (PIRs) based on asset-centric and risk-centric perspectives, enabling the translation of strategic business risks into operational intelligence directives.

2. **Operationalize the 5W3H Method:** Adapt the 5W3H methodology (22) to structure the Collection Plan, ensuring that intelligence requirements are comprehensive, measurable, and actionable.

3. **Automate Threat Data Filtering:** Implement the proposed methodology within a Threat Intelligence Platform (OpenCTI), using structured requirements to filter raw threat data and reduce the analytical overload caused by irrelevant information.

4. **Support Regulatory Compliance:** Demonstrate how the methodology contributes to compliance

with SFN regulatory requirements, including those established by Resolutions BCB 85/2021 and CMN 4.893/2021, as well as the 2025 updates (CMN 5.274 and BCB 538) (11, 12).

5. **Validate Methodological Effectiveness:** Quantitatively evaluate the reduction of data volume and the increase in informational density through a conceptual case study applied to the financial sector.

1.4 JUSTIFICATION

The relevance of this research can be justified from strategic, operational, and regulatory perspectives.

The systemic relevance of the SFN can be evidenced by the scale of its retail payment infrastructure. Official statistics indicate that PIX closed 2024 with approximately 63 billion transactions and approximately US$ 5.3 trillion transacted in the year (23), consolidating itself as the most used payment instrument in Brazil in volume and a critical component of day-to-day financial flows. In 2025, the Central Bank reported a new daily record of 313,339,828 PIX transactions (24), reinforcing the operational centrality and continuous exposure surface of this ecosystem. Given this magnitude, cyber incidents affecting financial service providers, payment rails, or supporting technology supply chains can rapidly propagate into cascading operational and economic impacts, strengthening the need for CTI practices that are continuously oriented by institutional priorities and auditable requirements.

Beyond transaction volume, economic impact indicators further demonstrate that cybersecurity constitutes a structural financial concern for the sector. According to the IBM Cost of a Data Breach Report 2025, the average cost of a data breach in Brazil reached US$ 1.22 million in 2025, with the financial sector remaining among the industries with the highest incident-related losses (25). In a system that processes trillions of dollars annually, even incidents below the global average cost threshold represent material operational and systemic risk. In parallel, industry data indicate that Brazilian banks allocated approximately US$ 8.7 billion to technology in 2025 (26), with a significant portion of these budgets directed to cybersecurity-related capabilities. In this context, a structured Direction and Planning approach for CTI is not merely a process improvement: it is a cost-effectiveness mechanism that increases informational density and reduces waste generated by indiscriminate collection, helping ensure that investments translate into actionable intelligence aligned with SFN risk profiles and regulatory traceability.

From a strategic standpoint, the protection of the SFN is essential to national stability. As highlighted by the ENSIC, disruptions in financial services may produce cascading social, economic, and political consequences (8). The critical nature of this protection was underscored by the C&M Software (CMSW) incident in June 2025, where the compromise of a critical provider led to massive illicit transfers via the PIX system, demonstrating the systemic risk inherent in the SFN's supply chain (27). By proposing a method that enhances threat anticipation through focused intelligence, this research contributes directly to the resilience of a critical national infrastructure.

From an operational perspective, cybersecurity teams increasingly face a paradox of data abundance and analytical scarcity. Analysts are required to process vast volumes of heterogeneous threat data, much of which lacks relevance to their specific organizational context (7). The proposed methodology addresses this challenge by introducing upstream filtering mechanisms that reduce noise before data reaches analytical workflows.

From a regulatory perspective, Brazilian financial institutions are subject to increasingly stringent governance requirements. While earlier resolutions required risk-based management, the 2025 regulatory updates demand specific actions of "Cyber Intelligence" and "Traceability", including explicit requirements for Cyber Intelligence actions, such as monitoring open sources, restricted environments, and illicit digital markets (13, 12). This dissertation provides a structured and auditable approach to aligning CTI practices with these modern regulatory obligations, transforming intelligence into a verifiable control.

Beyond its strategic and regulatory relevance, this dissertation offers three primary contributions to the field of Cyber Threat Intelligence. From a scientific perspective, it advances the state of the art by formalizing a structured and reproducible methodology for the Direction and Planning phase of the CTI cycle, a stage frequently acknowledged as critical in doctrine but insufficiently operationalized in academic and industrial practice. From an applied standpoint, it demonstrates how strategic risk definitions and Priority Intelligence Requirements can be systematically translated into automated filtering mechanisms within a Threat Intelligence Platform, effectively reducing informational noise while preserving contextual relevance. Finally, in contrast to prior works that predominantly emphasize post-collection processing, maturity assessment, or downstream enrichment techniques, this research introduces an upstream, governance-driven scoping approach that integrates regulatory compliance, asset criticality, and risk profiles into the core of intelligence production. This positioning differentiates the proposed approach by embedding governance, risk alignment, and auditability directly into the upstream phase of intelligence production.

1.5 CONTRIBUTIONS

The research conducted during this master's program resulted in the production and publication of two scientific papers that reflect the maturation of the proposed framework. These works demonstrate the evolution of the study from a methodological proposal to a validated, operational implementation applied to the context of the SFN.

The contributions are formalized through the following publications:

- **Methodological Proposal:** P. H. S. Gontijo, F. B. de Oliveira, R. de Oliveira Albuquerque, and J. J. Costa Gondim, "Structured Direction and Planning for Cyber Threat Intelligence in the Brazilian Financial System", in *10th Workshop on Communication Networks and Power Systems (WCNPS)*, IEEE, Brazil, 2025, DOI: 10.1109/WCNPS69127.2025.11295925.

  Contribution: This paper established the theoretical foundation of the research. It identified the gap in the Direction and Planning phase and proposed the initial framework. It focused on the strategic alignment between CTI processes and the risk profiles of financial institutions. The relevance and originality of this contribution were recognized with the Best Paper Award in the Communication Networks track.

- **Practical Operationalization and Validation:** P. H. S. Gontijo, R. de Oliveira Albuquerque, and J.

J. Costa Gondim, "Operationalizing Structured Direction and Planning for Cyber Threat Intelligence: A Practical Implementation for the Brazilian Financial System", in *IEEE International Conference on Big Data (IEEE BigData)*, China, 2025.

Contribution: This work validated the methodology through a conceptual case study using the OpenCTI platform. It demonstrated the technical operationalization of PIRs into lexical filtering and labeling rules. The study confirmed the efficacy of the method in managing informational noise: while the platform ingested the full baseline of 216,208 STIX objects, the automated scoping mechanism successfully classified and isolated only 903 objects as relevant to the SFN (a 99.58% reduction in analytical noise), ensuring that analysts focus solely on high-priority intelligence, even under the recently expanded collection mandates.

Synthesizing these outputs, the primary contributions of this dissertation to the field of Cyber Threat Intelligence include:

1. **A Structured Framework for Direction and Planning:** Unlike traditional approaches that focus on downstream data processing, this work provides a reproducible method for the upstream definition of requirements. It ensures that intelligence operations are driven by strategic intent, using PIRs to guide the automated operationalization of Threat Intelligence Platforms.
2. **Automated Scoping and Prioritization Mechanism:** The development of a classification pipeline that automatically tags and organizes incoming data based on its relevance to the institution. This mechanism applies progressive scoping labels (General, Global-Finance, SFN), effectively separating critical signals from generic noise and preventing information overload for the analytical team.
3. **Regulatory Alignment and Auditability:** The proposal provides a governance-oriented workflow that ensures CTI operations are traceable and compliant with the specific risk management mandates of the Brazilian National Financial System. By linking every relevant intelligence artifact back to a documented PIR, the methodology transforms CTI from an ad-hoc activity into an auditable process aligned with the institution's risk profile.

1.6 STRUCTURE OF THE DISSERTATION

This dissertation is organized into eight chapters, structured to provide a logical progression from the theoretical foundation and gap analysis to the methodological proposal, its technical implementation, results, and final discussions:

- **Chapter 1: Introduction** presents the contextualization of the theme, the motivation for the research regarding the SFN, the identified problem of informational noise in CTI, the objectives, and the justification for the study.
- **Chapter 2: Theoretical Foundation** establishes the necessary concepts regarding the Intelligence Cycle, Cyber Threat Intelligence, and Critical Infrastructure Protection. It specifically reviews the

regulatory landscape of the SFN, including the 2025 updates, to ground the asset and risk-centric approach.

- **Chapter 3: Related Work** analyzes the state of the art, categorizing existing approaches into post-collection processing, operational testing frameworks, and governance structures. It presents a comparative analysis to highlight the research gap.
- **Chapter 4: Methodology** describes the methodological approach adopted to achieve the research objectives and presents the structured methodology proposed for the DP phase. It introduces the five-stage model and explains how the 5W3H framework is operationalized to translate strategic risks and new regulatory requirements into explicit and auditable intelligence requirements.
- **Chapter 5: Implementation and Operationalization** describes the technical operationalization of the methodology. It details the laboratory environment, the automation middleware, and the construction of the rule-based filtering engine integrated with the OpenCTI platform.
- **Chapter 6: Experimental Results** presents the results obtained from the conceptual case study. It details the noise reduction metrics, analyzes retention rates by STIX object type, and validates the traceability and regulatory alignment of the retained intelligence with the updated requirements of the SFN.
- **Chapter 7: Discussion** interprets the operational and strategic implications of the results. It contrasts upstream scoping versus downstream scoring, discusses the benefits of continuous monitoring over episodic testing, and addresses the limitations of the study.
- **Chapter 8: Conclusion and Future Work** summarizes the main contributions of the research, synthesizes how the objectives were met, and outlines avenues for future development.

2 THEORETICAL FOUNDATION

This chapter establishes the conceptual and legal foundations necessary for the development of the proposed methodology. It begins by dissecting the classical doctrine of Intelligence and the Intelligence Cycle, establishing the theoretical lineage that underpins modern Cyber Threat Intelligence. Subsequently, it addresses the specificities of CTI, analyzing the technical standards for data representation (STIX) and transport (TAXII) not merely as formats, but as enablers of interoperability in a fragmented landscape. Finally, it contextualizes the research within the scope of Critical Infrastructure Protection (CIP), detailing the regulatory framework of the SFN that mandates the alignment between cybersecurity policies and institutional risk profiles, now reinforced by the latest directives.

2.1 THE NATURE OF INTELLIGENCE

In operational environments, particularly those involving critical services, the terms “data”, “information”, and “intelligence” are frequently—and erroneously—used interchangeably. Ideally, these concepts represent distinct stages in a value-generation chain, in which analytical processes progressively transform raw inputs into decision-relevant outputs. Data consists of raw, unevaluated signals or observations that have not yet been processed into meaning. Once organized or processed into a comprehensible form, data becomes information (2). However, information alone is insufficient for high-stakes decision-making, as it does not yet provide the contextual and evaluative refinement required to reduce uncertainty. Intelligence, in this sense, is the outcome of analysis that elevates information into decision-relevant judgments. This transformation process is conceptually illustrated in Figure 2.1, which depicts the progressive refinement of raw data into intelligence through analytical processing.

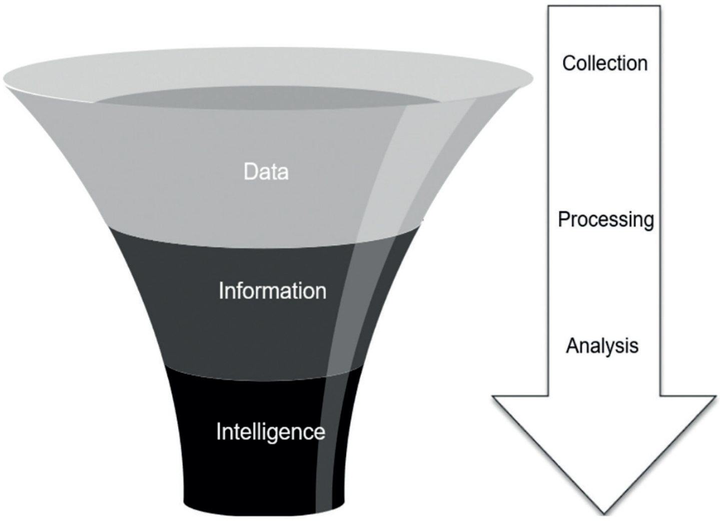


Figura 2.1: Transformation of data into intelligence through analytical processing. Source: (1).

Joint Publication 2-0 characterizes intelligence as a distinct product derived from the systematic processing, integration, evaluation, analysis, and interpretation of available information concerning adversaries, threats, or operational environments (15). It further emphasizes that intelligence is fundamentally estimative, with the primary purpose of reducing uncertainty and enabling decision advantage by clarifying what is known, what is unknown, and what is assessed as likely (15). In the context of cybersecurity, this distinction is critical: a feed of IP addresses is merely data; context regarding "who" is using those IPs and "why" constitutes intelligence. This transformation is characterized by a reduction in data volume and a corresponding increase in semantic and decision value.

To be operationally effective, intelligence must possess specific quality attributes: it must be anticipatory, timely, accurate, usable, complete, relevant, objective, and available (15, 17). Failing to meet these criteria—for instance, providing accurate intelligence that arrives too late to influence a decision—renders the output useless. The challenge in modern CTI is not the lack of data, but the inability to filter irrelevant data to produce these quality attributes (7), usually caused by limited processing capacity and the difficulty of handling large volumes of heterogeneous threat information.

2.2 THE INTELLIGENCE CYCLE

The intelligence cycle is the systematic process by which information is transformed into intelligence and delivered to consumers (16, 17). Although often depicted as a linear sequence, modern doctrine treats the cycle as a set of concurrent and iterative activities governed by feedback loops and changing requirements (15). A widely adopted representation defines four core phases: Direction and Planning, Collection, Analysis, and Dissemination (16). Some doctrinal models emphasize Evaluation and Feedback as continuous activities rather than a discrete step (2).

Figure 2.2 illustrates the intelligence core functions and their interactions. The model highlights that intelligence is not defined by collection volume, but by purposeful conversion of information into decision-support products, continuously refined through feedback.

2.2.1 Direction and Planning

Direction and Planning constitutes the governing phase of the cycle. It establishes "what" must be known (requirements), "why" it must be known (rationale), and "how" resources will be allocated to acquire that knowledge (18). According to the UK Ministry of Defence (2), this phase is critical because it prioritizes the commander's uncertainties. Without structured direction, the subsequent phases risk collecting irrelevant data, leading to informational noise and “analysis paralysis” (7).

In the context of this work, this phase is where the institution's risk profile is translated into Priority Intelligence Requirements. Failure in this phase cascades through the entire cycle; if the direction is vague, collection becomes indiscriminate, processing and analysis become overwhelmed, and the final intelligence product fails to support decision-making (14). As Osliak et al. (28) argue, effective security management requires policy reevaluation, which must be driven by structured requirements defined in this phase.

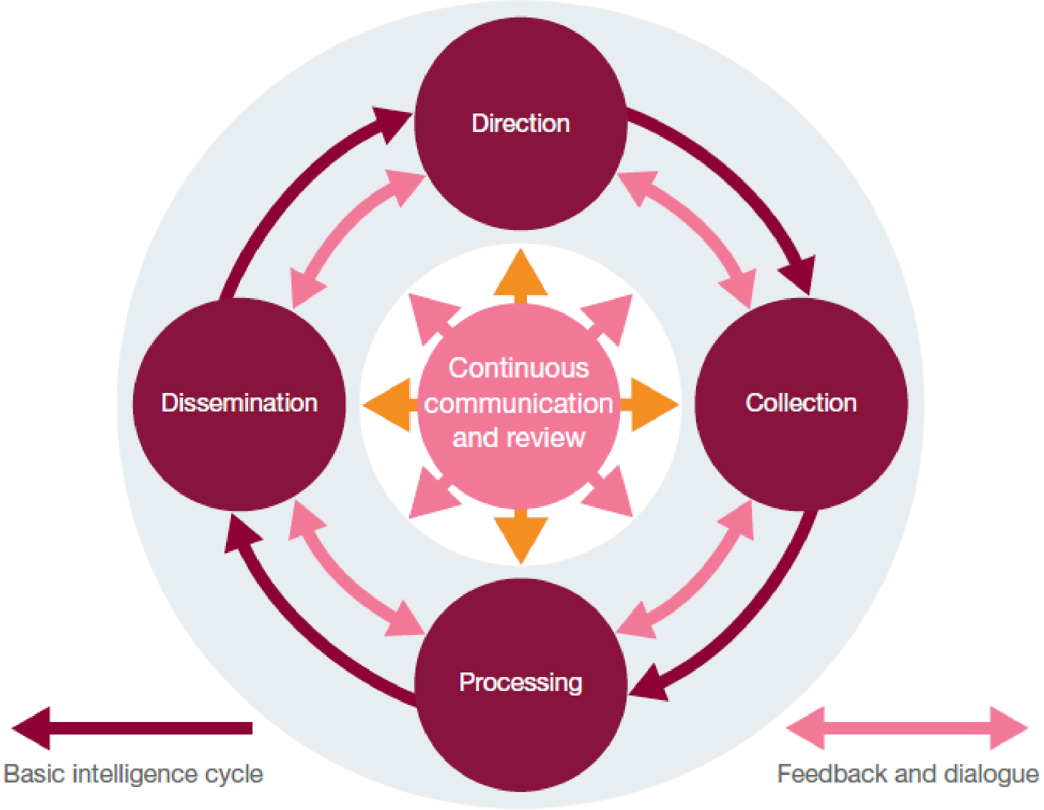


Figura 2.2: The Intelligence Cycle. Source: (2).

2.2.2 Collection

Collection involves the acquisition of raw data to satisfy the requirements defined in the Direction phase. Sources may include Open Source Intelligence (OSINT), Human Intelligence (HUMINT), Signals Intelligence (SIGINT), and others (15). In the modern CTI context, collection often involves ingesting data feeds from external vendors, sharing communities (CSIRTs/ISACs), or internal telemetry (29).

Effective collection is not about gathering all available data, but gathering the right data. As noted by Faiella et al. (30), one of the weakest points in current security detection systems is the retrieval of data from OSINT due to its unstructured nature. Without the filters established in the Direction phase, the Collection phase can easily become a bottleneck, flooding the system with high volumes of low-fidelity indicators (7).

2.2.3 Processing and Analysis

Processing converts raw data into a format suitable for analysis (e.g., decryption, translation, normalization, and correlation). Analysis is the cognitive process of evaluating and integrating information to create knowledge (15). In automated CTI systems, this phase includes the correlation of events and the enrichment of indicators with contextual data.

Faiella et al. (30) emphasize that in order to improve quality, information should be correlated with real-time data coming from the monitored infrastructure. This allows for the evaluation of a “threat score” through heuristic-based analysis, prioritizing threat detection and incident response. For example, raw data might indicate an external IP address scanning a network port. Processing normalizes this log entry. Analysis, however, correlates this scan with threat intelligence feeds to identify that the IP belongs to a known APT group targeting financial institutions, thereby elevating the event from a generic “scan” to a “targeted reconnaissance effort” (14).

2.2.4 Dissemination

Dissemination is the timely conveyance of intelligence to the user in a usable form. Effective dissemination ensures that the right intelligence reaches the right person at the right time to support a decision (15). This implies that the format must be tailored to the consumer; a CISO requires a strategic brief on risk exposure, whereas a SOC analyst requires machine-readable IoCs (e.g., STIX/TAXII) for immediate implementation in security controls (28, 31).

2.2.5 Evaluation and Feedback

This phase assesses whether the intelligence satisfied the requirement. It closes the loop, allowing the refinement of requirements and the adjustment of the collection plan for future cycles (2). In the context of this dissertation, feedback is essential to tune the PIRs, ensuring that the noise reduction filters remain effective as the threat landscape evolves.

2.3 INTELLIGENCE REQUIREMENTS MANAGEMENT

Intelligence Requirements Management (IRM) is the sub-discipline within the Direction and Planning phase responsible for validating, prioritizing, and managing the information needs of the organization (18). It bridges the gap between the abstract needs of the decision-maker and the concrete actions of the collector.

2.3.1 Priority Intelligence Requirements

A Priority Intelligence Requirement is an intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or the operational environment (15, 18). PIRs drive the intelligence cycle; if a collection activity does not map to a PIR, it is theoretically a waste of resources.

In the methodology proposed by this work, PIRs are used as the primary “gatekeeper” or filter to separate signal from noise. By defining PIRs based on the intersection of critical assets and relevant threats, the organization ensures that it only collects data that matters to its specific risk profile (20).

2.3.2 Requests for Information and Indicators

PIRs are often high-level strategic questions (e.g., “Is an APT targeting our payment switch?”). To be answered, they must be decomposed into Specific Information Requirements (SIRs) or Requests for Information (RFIs). These are granular questions that can be answered by specific data points or Indicators (18).

An indicator is an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action (15). In CTI, indicators are often technical artifacts (IoCs), but in a mature intelligence process, they are merely the evidence used to answer the broader RFI (7).

2.3.3 Collection Planning and Strategy

The collection plan is the artifact that connects requirements to resources. It operationalizes the PIRs by assigning specific collection tasks to specific assets (18). A robust collection plan ensures that the organization is not merely “gathering data” but actively “hunting” for the answers to its strategic questions (20). This systematic approach transforms CTI from a reactive feed-consumption model to a proactive, hypothesis-driven operation.

2.4 CYBER THREAT INTELLIGENCE

CTI is the application of intelligence doctrine to the domain of cybersecurity. It is defined as evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets (7). Cyber Threat Intelligence moves beyond simple “threat data” (e.g., a list of bad IPs) by adding context: who is attacking, why, and how.

2.4.1 Levels of Cyber Threat Intelligence

To be effective, Cyber Threat Intelligence must be tailored to the specific needs of its audience, ranging from senior executives to network defenders. While traditional intelligence doctrine often delineates levels based on the scope of military operations, the framework proposed by the Council of Registered Ethical Security Testers (CREST) categorizes CTI into three distinct levels based on the nature of the material, its intended audience, and its application: Strategic, Operational, and Tactical (1), as illustrated in Figure 2.3.

2.4.1.1 Strategic

Strategic intelligence is designed to inform senior decision-makers, such as the C-Suite and board members, about broader changes in the threat landscape. It focuses on business risk rather than technical terminology, often covering long-term trends, geopolitical developments, and the financial impact of cyber activities. This level of intelligence assists organizations in shaping their long-term security strategy, allocating budgets, and understanding how adversarial motives align with organizational objectives (1).

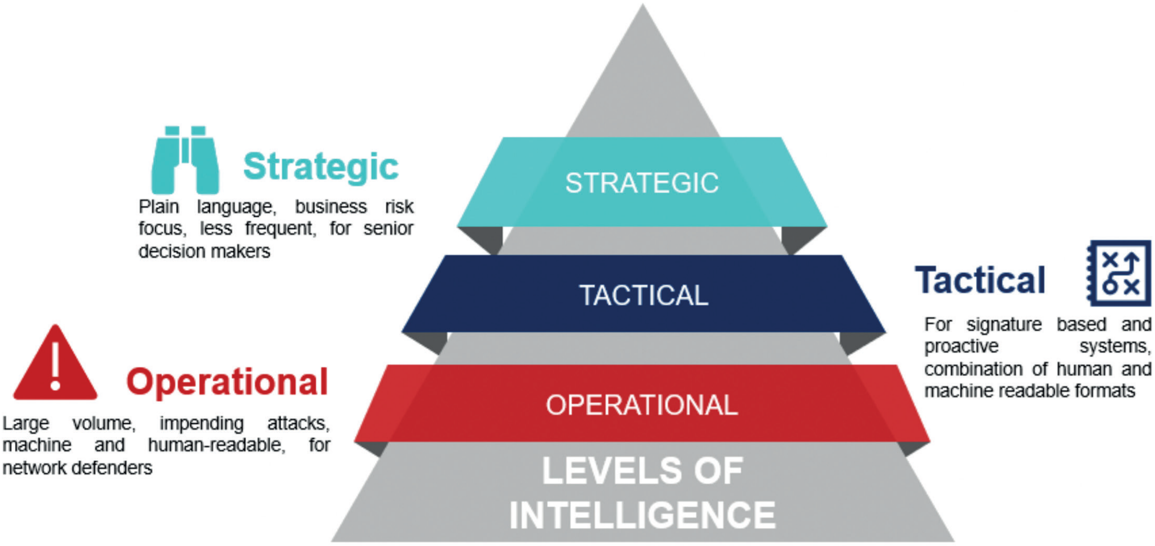

Strategic
Plain language, business risk focus, less frequent, for senior decision makers
STRATEGIC
TACTICAL
Tactical
For signature based and proactive systems, combination of human and machine readable formats
Operational
Large volume, impending attacks, machine and human-readable, for network defenders
OPERATIONAL
LEVELS OF INTELLIGENCE

Figura 2.3: Levels of Cyber Threat Intelligence. Source: (1).

2.4.1.2 Tactical

Tactical intelligence focuses on the TTPs used by threat actors, as well as the technical artifacts associated with their attacks. This level encompasses IoCs—such as IP addresses, file hashes, and domain names—which are essential for updating signature-based defense systems and supporting Security Operations Centers (1). While some academic frameworks distinguish a separate "Technical" level for these atomic indicators, CREST integrates them into the Tactical level, emphasizing their utility for network defenders in detecting and responding to known attack types and conducting proactive threat hunting (1).

2.4.1.3 Operational

According to the CREST framework, Operational CTI relates to details of potential impending operations against an organization. This level of intelligence provides insight into specific campaigns or attacks that may be imminent, often derived from sources such as "chatter" among hacktivists or data leaked on underground forums (1). Operational intelligence helps security managers understand the specific nature of threats targeting the organization, allowing for the prioritization of defensive resources against the most relevant adversaries.

2.4.2 Technical Threat Intelligence and Enrichment

Technical CTI focuses on the identification of specific IoCs such as malicious IP addresses, URLs, and file hashes. However, raw IoCs often lack context and suffer from high false-positive rates. "Enrichment" is the process of augmenting these indicators with additional data (e.g., geolocation, threat actor attribution, associated malware families, passive DNS history) to increase their confidence and utility (30).

Faiella et al. (30) present an Enriched Threat Intelligence Platform (ETIP) approach, highlighting that enrichment is crucial for calculating a “threat score” that aids in prioritization. They argue that correlating static OSINT data with dynamic real-time data from the monitored infrastructure is essential to produce valuable intelligence. However, they also note that processing vast amounts of unstructured OSINT data is a significant bottleneck, reinforcing the need for the upstream filtering proposed in this dissertation.

2.4.3 Standardization

To enable the automated exchange of Cyber Threat Intelligence and ensure interoperability across heterogeneous security ecosystems, standardized representation languages and transport protocols are essential. In this context, the OASIS standards STIX and TAXII constitute the de facto global reference for structuring and sharing CTI in a machine-readable and interoperable manner.

- **STIX (Structured Threat Information Expression):** STIX is a standardized language developed by OASIS for representing Cyber Threat Intelligence in a structured and machine-readable format. The STIX 2.1 specification defines a comprehensive data model composed of eighteen STIX Domain Objects (SDOs), two Relationship Objects (SROs), and Cyber-observable Objects (SCOs), enabling the consistent representation of threat actors, attack patterns (TTPs), malware, tools, vulnerabilities, campaigns, and observed data (32). By explicitly modeling relationships between entities, STIX supports the construction of graph-based intelligence representations, transforming isolated indicators into contextualized and analyzable knowledge structures.
- **TAXII (Trusted Automated Exchange of Intelligence Information):** TAXII is an application-layer protocol standardized by OASIS to support the secure and automated exchange of CTI over HTTPS. The TAXII 2.1 specification defines a set of RESTful services and message exchanges—such as collections, channels, and discovery services—that enable organizations to publish, consume, and synchronize STIX-formatted intelligence across organizational and sectoral trust boundaries (33). TAXII decouples intelligence production from consumption, allowing scalable and controlled information sharing without requiring bilateral integrations.

2.4.4 Threat Intelligence Platforms

To manage the volume and complexity of CTI data, organizations utilize Threat Intelligence Platforms. A TIP acts as a central repository that aggregates, correlates, and analyzes threat data from multiple sources in real-time. Faiella et al. (30) discuss how TIPs like MISP allow for the storage and sharing of IoCs but often require additional modules for effective enrichment and scoring. Modern TIPs, such as OpenCTI, support the STIX standard natively and allow for the automation of the intelligence cycle. However, without a structured methodology for "what" to ingest (Direction & Planning), a TIP can easily become a “data swamp” rather than an intelligence hub (14).

2.5 CRITICAL INFRASTRUCTURE PROTECTION

Critical Infrastructures are defined as assets, systems, or networks, whether physical or virtual, so vital to a nation that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health, or safety (4, 34). In the Brazilian context, the protection of these infrastructures has evolved from a decentralized concern into a structured State policy, governed by a hierarchical framework of decrees that establishes CTI not merely as a technical capability, but as a strategic necessity for national sovereignty.

2.5.1 The Brazilian National Policy and Strategy

The governance of CIP in Brazil is anchored in the National Policy for Critical Infrastructure Security, established by Decree No. 9.573/2018 (4). This decree provides the legal definition of CIs in Brazil, characterizing them as installations, services, goods, and systems whose disruption or destruction causes serious social, environmental, economic, political, or international impact, or affects the security of the State and society. The PNSIC establishes the principle of "integration" mandating cooperation between government agencies, the private sector, and society. Crucially for this work, the policy explicitly lists the "integration of data regarding threats" as a specific objective, validating the need for structured intelligence methodologies (4).

Building upon the policy, Decree No. 10.569/2020 approved the National Strategy for Critical Infrastructure Security (8). While the policy defines "what" must be protected, the strategy defines "how". The ENSIC introduces the concept of interdependence, recognizing that a cyber incident in the financial sector can trigger cascading effects across energy, telecommunications, and transportation sectors. The strategy is built upon "structuring axes", one of which is "Data and Information Management". This axis explicitly demands the selection, organization, and qualification of data to support strategic decision-making, directly aligning with the objectives of the Direction and Planning phase of CTI proposed in this dissertation (8).

Operationalizing this strategy, Decree No. 11.200/2022 approved the National Plan for Critical Infrastructure Security (35). This document represents the executive layer of the framework, establishing specific actions and deadlines. A key component of PLANSIC is the mandate to implement an "Integrated Data System for Critical Infrastructure Security". This system aims to centralize risk analyses and threat mapping, reinforcing that isolated data silos are insufficient for protecting national interests. The plan assigns specific responsibilities to the Ministry of Economy to coordinate sectoral plans for the financial area, ensuring that cybersecurity efforts are not generic but tailored to the sector's specificities (35).

Completing the macro-regulatory framework, Decree No. 11.856/2023 instituted the National Cybersecurity Policy (5). This recent decree elevates cybersecurity to a matter of national sovereignty. Unlike previous general infrastructure regulations, PNCiber specifically addresses the cyber domain. Its principles include the "prevention of incidents and cyber attacks, particularly those directed at national critical infrastructures" (5).

PNCiber explicitly lists as an objective the "promotion of information exchange" regarding cyber threats among the Union, the private sector, and society. By establishing the National Cybersecurity Committee

(CNCiber), the decree creates a governance layer that requires institutions to move beyond reactive security postures toward predictive and resilient capabilities. This reinforces the argument that CTI programs in the SFN must be structured and auditable, as they contribute to a broader national defense mechanism (5).

2.5.2 The Financial Sector as a Priority Domain

Within the CIP framework, the SFN is classified as a priority domain due to its high degree of digitalization and its central role in the country's economic stability (6, 8). The interconnectivity of the SFN means that it is not merely a target for financial fraud but a vector for systemic instability.

To address these specific risks, the National Monetary Council (CMN) and the Central Bank of Brazil (BCB) have issued stringent regulations that function as the sectoral application of the national strategies described above. In December 2025, this framework reached a new level of technical prescription with the update of the following resolutions:

- **Resolution CMN No. 5.274/2025 (amending CMN No. 4.893/2021):** This resolution establishes the cybersecurity policy for financial institutions. While Article 2 remains the core mandate for risk-based policies, the 2025 update introduces a list of 14 mandatory procedures and controls (11). Crucially, it now explicitly demands "cyber intelligence actions", including the monitoring of information on the Internet, Deep Web, and Dark Web (12, 13). This requirement validates the methodology of this dissertation, as it necessitates a structured planning phase to manage the scope of such expanded monitoring.
- **Resolution BCB No. 538/2025 (amending BCB No. 85/2021):** Applying to payment institutions, this resolution mirrors the prescriptive requirements for infrastructure protection and incident response (12). It emphasizes the need for traceability and the implementation of controls to reduce vulnerability, including mandatory annual intrusion tests performed by independent companies (12). The 2025 framework treats the communication infrastructure of the RSFN (Brazilian National Financial System Network, *Rede do Sistema Financeiro Nacional*), which interconnects financial institutions and supports critical services such as the PIX instant payment system and the STR (Reserve Transfer System), as critical infrastructure, requiring physical and logical isolation when operating in cloud environments (11, 12).

Furthermore, BCB Normative Instruction No. 664/2025 provides the technical roadmap for these intelligence actions, detailing the requirement to monitor "information of interest" (such as leaked credentials, vulnerabilities, and keys) across the surface and dark web, as well as private communication groups (13). This legal landscape transforms the Direction and Planning phase from a "best practice" into a mandatory technical audit trail. Without the structured Priority Intelligence Requirements proposed in this work, institutions would struggle to demonstrate the "traceability" and "compatibility with risk profile" explicitly demanded by the regulator under the new regulatory context. (12, 11).

In summary, the theoretical foundation for this work is grounded in a robust and increasingly prescriptive legal hierarchy. From the National Policy down to the sectoral resolutions introduced in 2025, there is a clear mandate for structured, risk-based, and highly technical intelligence practices to protect the nation's critical financial infrastructure.

3 RELATED WORK

This chapter presents a critical review of the state-of-the-art regarding Cyber Threat Intelligence, positioning the proposed methodology within the broader academic and operational landscape. To demonstrate the specific gap addressed by this dissertation, the literature is analyzed in four distinct streams of research that have attempted to solve the challenges of CTI management: (i) Post-Collection Processing and Enrichment; (ii) Operational Testing Frameworks; (iii) Governance and Maturity Models; and (iv) Advanced Analytical Models. Each stream provides valuable contributions to the field but leaves specific gaps regarding the upstream reduction of informational noise through structured Direction and Planning, particularly within the regulatory context of the SFN, as redefined by the prescriptive mandates introduced under the 2025 regulatory agenda.

3.1 POST-COLLECTION PROCESSING AND ENRICHMENT APPROACHES

The most prolific stream of CTI research addresses the challenge of information overload by focusing on the "downstream" phases of the intelligence cycle—specifically Processing and Analysis. These approaches accept large volumes of data ingestion as a premise and seek to mitigate noise through retrospective scoring, correlation, or enrichment.

Faiella et al. (30) propose the "Enriched Threat Intelligence Platform". Their architecture is significant for integrating Open Source Intelligence with internal telemetry to calculate a dynamic “threat score.” This scoring mechanism effectively prioritizes alerts that have already entered the Security Operations Center (SOC), providing a robust method for managing incidents (30). However, the limitation of this approach lies in its position within the cycle: it treats noise as a processing problem rather than a collection planning problem. By filtering data only after it has been ingested, organizations still incur the computational and cognitive costs of handling irrelevant data.

Similarly, Silva et al. (14) propose a methodology for improving CTI quality through an IoC enrichment process. Their work is particularly relevant to this dissertation as it also employs the 5W3H framework (What, Who, Why, When, Where, How, How Much, How Long) to create situational awareness (14). However, Silva et al. apply 5W3H primarily as an analytical tool to enrich data after collection. In contrast, the methodology proposed in this dissertation shifts the application of 5W3H to the Direction and Planning phase, using it to define what should be collected in the first place, thereby reducing the impact of low-value artifacts on the analytical process.

Sector-specific platforms have also been explored to address relevance. Leszczyna and Wróbel (29) present a threat intelligence platform tailored for the energy sector, introducing mechanisms for anonymization and trust circles. While their work validates the importance of sectoral context—a principle shared by this dissertation regarding the financial sector—their primary focus is on the architecture of dissemination and sharing between entities, rather than the internal methodology for defining and filtering collection requirements based on risk (29).

3.2 OPERATIONAL TESTING FRAMEWORKS (THREAT-LED DEFENSE)

A second stream of literature, heavily influenced by central banks and regulators, operationalizes CTI through Threat-Led Penetration Testing (TLPT). Prominent examples include the European Central Bank's TIBER-EU (36) and the Bank of England's CBEST (37).

These frameworks represent a mature application of the Direction phase. They explicitly require the production of a "Targeting Report" and a "Threat Intelligence Report" to define the scope of red teaming exercises. Thus, they successfully link strategic risks to technical testing scenarios (36, 37). However, these frameworks are designed for episodic validation rather than continuous monitoring. In the current SFN landscape, the Resolution BCB No. 538/2025 now mandates annual intrusion tests performed by independent companies, requiring a continuous feed of relevant threats to inform these tests (12). While they prove the concept of intelligence-led scoping, they do not provide a mechanism for the daily, automated management of threat feeds required for continuous defensive operations, leaving a gap for methodologies that apply similar rigor to daily CTI operations.

3.3 GOVERNANCE, MATURITY, AND EVALUATION MODELS

Recognizing that technology alone cannot solve intelligence challenges, a third stream focuses on governance structures. Lopez and Awad (20) provide a comprehensive framework for establishing a threat intelligence program, emphasizing the alignment of CTI with business objectives. Their work confirms the necessity of the Direction and Planning phase but remains descriptive at the managerial level, not prescribing the technical mechanisms to translate requirements into platform filtering rules (20).

In terms of maturity assessment, the "CTI Capability Maturity Model" (CTI-CMM) (21) offers a structured approach to measuring people, processes, and technology. It defines the "what" of a mature program—such as the existence of Priority Intelligence Requirements—but does not detail the "how" of their technical operationalization (21).

Complementing these governance models, Melo e Silva et al. (31) propose a methodology to evaluate CTI standards (like STIX) and platforms (like MISP and OpenCTI). Their analysis uses 5W3H to assess the completeness of these tools. This dissertation builds upon their evaluation by selecting OpenCTI as the implementation environment, but moves beyond evaluation to propose a specific configuration methodology that forces these platforms to operate according to a risk-centric logic.

Within the Brazilian context, the regulatory update of 2025 (Resolution CMN No. 5.274) shifted the governance paradigm from a flexible "risk-based" approach to a prescriptive one, mandating 14 specific technical controls (11). This regulatory evolution highlights a gap in current maturity models, which often fail to account for the deterministic auditability required by the Central Bank's new technical standards for "Cyber Intelligence Actions" (13)

3.4 ADVANCED ANALYTICAL MODELS

Finally, recent research has explored advanced data science techniques to infer relationships in CTI. Zhang et al. (38) propose a "Requirement-Cyber Threat Intelligence knowledge graph" (RCTI) using Edge Propagation Graph Neural Networks (EGNN). Their work demonstrates the potential of predicting links between security requirements and threat intelligence data. Similarly, Mouratidis et al. (39) introduce a modelling language for security incident handling.

These contributions represent the cutting edge of analytical reasoning. However, they rely on complex probabilistic models applied to existing datasets to infer knowledge, requiring significant computational resources and high processing capacity. In the specific context of the SFN, governed by strict regulatory requirements for auditability and traceability, there is a preference for deterministic, rule-based approaches. Furthermore, emerging threats, such as "vibe hacking" (AI-assisted intrusions), require immediate and explainable filtering that probabilistic models may struggle to justify during a regulatory audit (40). The gap here is not in the sophistication of analysis, but in the application of structured, deterministic filtering that ensures compliance and explainability before advanced analytics are applied.

3.5 COMPARATIVE ANALYSIS

The critical review of the literature reveals that while individual components of the intelligence cycle are well-addressed, there is a lack of a unified methodology that integrates strategic Direction and Planning with technical automation to prevent information overload upstream.

To objectively demonstrate this gap and the specific contribution of this dissertation, Table 3.1 compares the proposed methodology against key related works. The comparison is based on four critical criteria derived from the specific challenges of the SFN:

1. **Direction & Planning Focus:** Does the work primarily address the upstream definition of requirements (PIRs/RFIs)?
2. **Upstream Filtering:** Does the method reduce data noise before or during ingestion, rather than relying on post-ingestion scoring or enrichment?
3. **Deterministic Automation:** Is the method translatable into automated technical rules (e.g., regex, tags) suitable for continuous operations, as opposed to manual analysis or episodic testing?
4. **SFN Regulatory Alignment:** Does the work explicitly address the risk-profiling and governance requirements of the Brazilian context?

Tabela 3.1: Comparative Analysis of Related Works and the Proposed Methodology

Related Work	**DP Focus**	**Upstream Filtering**	**Determ. Automation**	**SFN Alignment**
Tounsi & Rais (7)	No	No	No	No
Faiella et al. (ETIP) (30)	No	No (Scoring)	Yes	No
Silva et al. (14)	No	No (Enrichment)	Partial	No
Melo e Silva et al. (31)	No	No	No	No
TIBER-EU (36) / CBEST (37)	Yes	N/A	No (Manual)	No
Leszczyna & Wróbel (29)	No	No	Yes	No
Lopez & Awad (20)	Yes	No	No	No
Zhang et al. (EGNN) (38)	No	No	No (Probabilistic)	No
Mouratidis et al. (39)	No	No	Yes	No
Osliak et al. (28)	No	No	Yes	No
CTI-CMM (21)	Yes	No	No	No
Proposed Methodology	**Yes**	**Yes**	**Yes**	**Yes**

As evidenced in Table 3.1, a clear dichotomy emerges in the current state of the art. Works such as Lopez (20) and the TIBER-EU framework (36) demonstrate a strong focus on the Direction and Planning phase, establishing the necessary governance to define what intelligence is required; however, they rely heavily on manual processes and episodic validation, lacking the mechanisms for continuous, automated operation. Conversely, technical contributions like Faiella et al. (30) and Zhang et al. (38) provide robust deterministic automation, but their application is predominantly downstream, focusing on processing or scoring data only after it has already been ingested.

This dissertation bridges this specific gap by integrating the governance rigor of the DP phase with the efficiency of technical automation. It proposes a methodology that operationalizes strategic requirements into automated filtering rules before collection occurs, thereby achieving upstream noise reduction. Furthermore, unlike generalist approaches, this methodology is explicitly tailored to the regulatory mandates of the SFN, ensuring that the resulting intelligence is not only technically manageable but also compliant with the sector's new prescriptive and auditable obligations.

4 METHODOLOGY

In response to the gap identified in the literature and the objectives outlined in Chapter 1, this chapter presents the core contribution of this dissertation: a structured methodology for the Direction and Planning phase. It details the research design and introduces a five-stage framework—ranging from Strategic Alignment to the Collection Plan using an adapted 5W3H model. This methodological artifact is designed to transform abstract institutional risks and prescriptive regulatory mandates into deterministic intelligence requirements, ensuring that subsequent collection activities are auditable and strictly aligned with the institution's risk profile, as required by the regulatory framework.

4.1 METHODOLOGICAL OVERVIEW

To achieve the general and specific objectives, this research adopted an applied methodological approach, combining qualitative analysis of doctrine and regulations with experimental validation of technical artifacts. The research design was structured into three interdependent phases:

1. **Phase 1: Conceptual Framework Development.** This phase involved the qualitative analysis of the normative framework for Critical Infrastructure Protection and cybersecurity—specifically the National Plan for Critical Infrastructure Security (Decree No. 11.200/2022) (35), National Policy for Critical Infrastructure Security (Decree No. 9.573/2018) (4), National Strategy for Critical Infrastructure Security (Decree No. 10.569/2020) (8), and the National Cybersecurity Policy (Decree No. 11.856/2023) (5)—alongside sector-specific financial regulations, including Resolutions CMN 4.893/2021 and BCB 85/2021, and their subsequent prescriptive updates, Resolution CMN No. 5.274/2025 and Resolution BCB No. 538/2025 (11, 12). Combined with classical intelligence doctrine, this analysis aimed to define the five stages of the proposed model.
2. **Phase 2: Technical Operationalization.** This phase focused on translating the conceptual model into executable mechanisms. It involved the development of a Python-based automation layer integrated with the OpenCTI platform to convert Priority Intelligence Requirements into deterministic filtering rules. This implementation is detailed in Chapter 5.
3. **Phase 3: Experimental Validation.** The final phase consisted of a quantitative case study using a baseline dataset of over 216,000 SDOs. The efficacy of the proposed methodology was measured through metrics of noise reduction and informational density, as presented in Chapter 6.

4.2 PROPOSED STRUCTURED DIRECTION AND PLANNING MODEL

The Direction and Planning phase constitutes the foundation of the intelligence cycle. However, as evidenced in the literature review, this phase is frequently under-applied in operational settings, where efforts tend to concentrate on downstream activities such as collection, analysis and information sharing. This imbalance contributes directly to the phenomenon of information overload, in which analysts are exposed to high volumes of low-fidelity data that do not map to institutional risks or decision needs (7).

To address this gap in the context of the SFN, this dissertation proposes a structured five-stage methodology designed to transform institutional risks and regulatory mandates into explicit and technically operational requirements. The method shifts the CTI paradigm from volume-centric ingestion to risk-centric scoping, so that every collected element has a defined purpose, traceability, and justification.

The proposed methodology is grounded in the principle that intelligence requirements must be asset- and risk-centric, enabling alignment with risk-profile obligations and the 14 mandatory procedures and controls imposed on financial institutions by the 2025 regulatory framework updates(11). In practical terms, this means that the intelligence enterprise is scoped by what must be protected and why, before deciding what to collect and how to operationalize it.

Figure 4.1 summarizes the sequential flow of the Direction and Planning model, emphasizing end-to-end traceability from governance-level needs to tactical collection directives and implementation artifacts.

The model comprises five integrated stages:

1. **Strategic Alignment:** definition of critical assets and functions based on institutional context and the new regulatory requirements.
2. **Threat Mapping:** identification of threat classes relevant to the protected assets, using sector-oriented threat baselines.
3. **Priority Intelligence Requirements definition:** formulation of high-level intelligence questions derived from the asset–threat intersection.
4. **Requests for Information formulation:** decomposition of each Priority Intelligence Requirement into granular and collectible information needs.
5. **Collection Plan development:** operationalization of requirements using a structured specification model based on 5W3H.

4.3 STAGE 1: STRATEGIC ALIGNMENT

Stage 1 establishes the foundational scope of the intelligence program by defining "what" must be protected and "why". In contrast to generic CTI implementations that ingest broad and sector-agnostic threat feeds, this stage constrains the intelligence scope to the institution’s critical functions and assets, in accordance with its operational context and regulatory risk profile.

Within the Brazilian National Financial System, critical assets encompass both intangible and tangible components that directly support essential financial services. From a governance perspective, this stage operationalizes the regulatory requirement that cybersecurity policies be compatible with the institution’s risk profile, while specifically addressing the Article 3-A of Resolution CMN 5.274/2025 (11, 12).

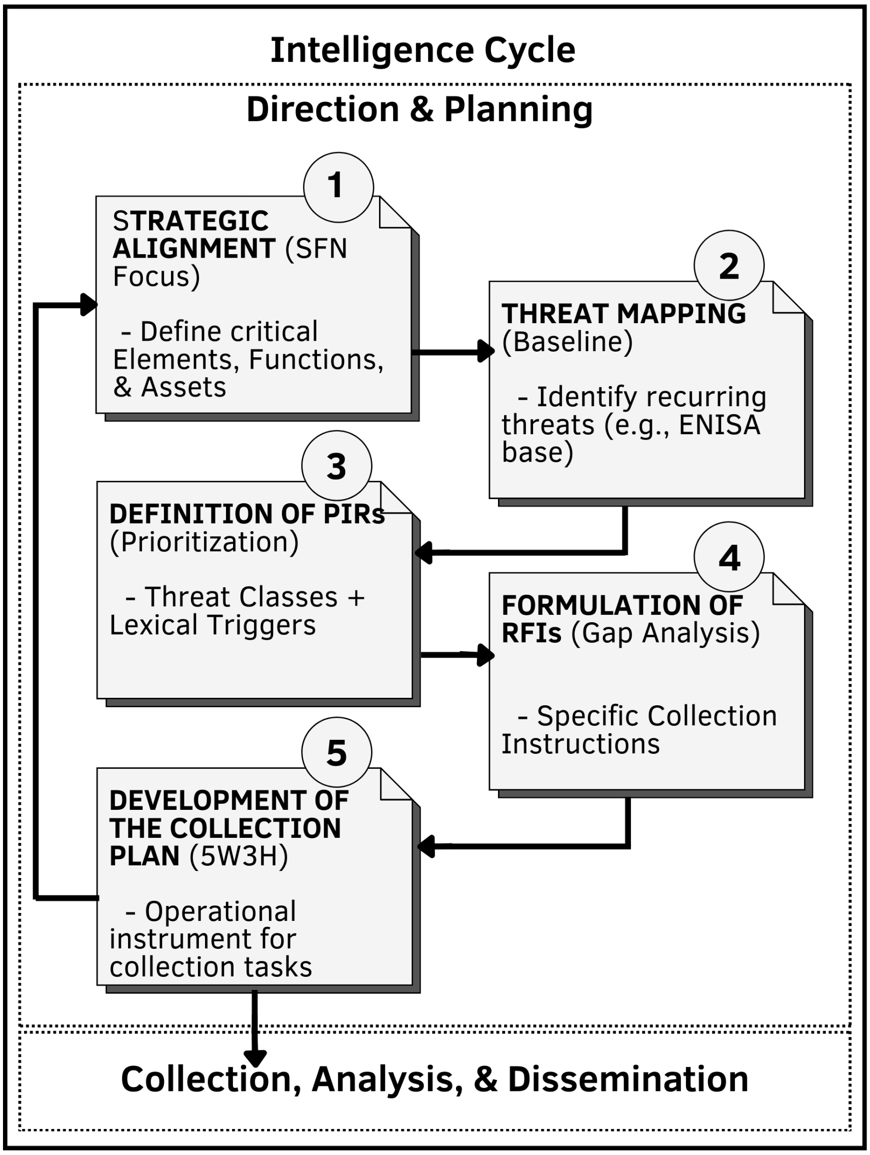

Intelligence Cycle
Direction & Planning
1
STRATEGIC ALIGNMENT (SFN Focus)
- Define critical Elements, Functions, & Assets
2
THREAT MAPPING (Baseline)
- Identify recurring threats (e.g., ENISA base)
3
DEFINITION OF PIRs (Prioritization)
- Threat Classes + Lexical Triggers
4
FORMULATION OF RFIs (Gap Analysis)
- Specific Collection Instructions
5
DEVELOPMENT OF THE COLLECTION PLAN (5W3H)
- Operational instrument for collection tasks
Collection, Analysis, & Dissemination

Figura 4.1: Proposed structured methodology for Direction and Planning. Source: Author

To support traceability and practical adoption, assets are grouped into high-level classes. Table 4.1 illustrates examples of critical asset classes relevant to the SFN.

The output of Stage 1 is a formally documented set of critical asset classes and functions, acting as a persistent scoping reference.

4.4 STAGE 2: THREAT MAPPING

While Stage 1 defines what must be protected, Stage 2 identifies what threatens it. To avoid arbitrary selection of threat topics, this dissertation adopts a documentary, sector-oriented approach based on threat landscape reports and financial-sector threat reviews. For the construction of a baseline threat taxonomy, five financial-sector references covering the 2023–2025 horizon were analyzed:

Tabela 4.1: Illustrative classes of critical assets in the SFN

Asset Class	Examples
Payment and settlement systems	PIX infrastructure (isolated instances), STR environments, interbank transfer systems, SWIFT gateways
Customer and financial data	Customer databases, transaction histories, credit records, personally identifiable information
Digital service channels	Internet banking platforms, mobile banking applications, APIs exposed to partners
Supporting infrastructure	RSFN communication services, authentication services, identity providers, cloud-hosted workloads, PSTI integrations

1. Financial Services Information Sharing and Analysis Center: "Navigating Cyber 2025 Annual Threat Review and Predictions" (41);

2. Federal Reserve Board: "Cybersecurity and Financial System Resilience Report 2024" (42);

3. Office of the Comptroller of the Currency: "Cybersecurity and Financial System Resilience Report 2025" (43);

4. Nordic Financial CERT: "Cyber Threat Landscape for the Nordic Financial Sector 2025" (44);

5. European Union Agency for Cybersecurity: "Threat Landscape: Finance Sector 2024" (3).

Among these, the ENISA finance-sector taxonomy was selected as the primary reference because it provides a consolidated and structured classification of incidents into recurring threat classes (e.g., distributed denial-of-service, data-related threats, social engineering), which can be mapped to requirements and later operationalized as deterministic filtering triggers (3).

Figure 4.2 presents the distribution of threat categories reported by ENISA for the finance sector, which serves as the baseline reference for the threat taxonomy adopted in this stage.

Crucially, the regulatory framework, through *Instrução Normativa* BCB No. 664, now mandates that threat mapping includes "cyber intelligence actions" targeting information of interest across the surface web, Deep Web, Dark Web, and private communication groups (13). This stage outputs a Baseline Threat Taxonomy that incorporates these mandatory collection domains.

4.5 STAGE 3: PRIORITY INTELLIGENCE REQUIREMENTS DEFINITION

Stage 3 formalizes Priority Intelligence Requirements as the core output of Direction and Planning. In this methodology, PIRs are derived strictly from the intersection between the protected scope defined in Stage 1 and the relevant threat classes defined in Stage 2. Each PIR represents a decision-oriented question about a threat class that could materially impact a critical asset or function.

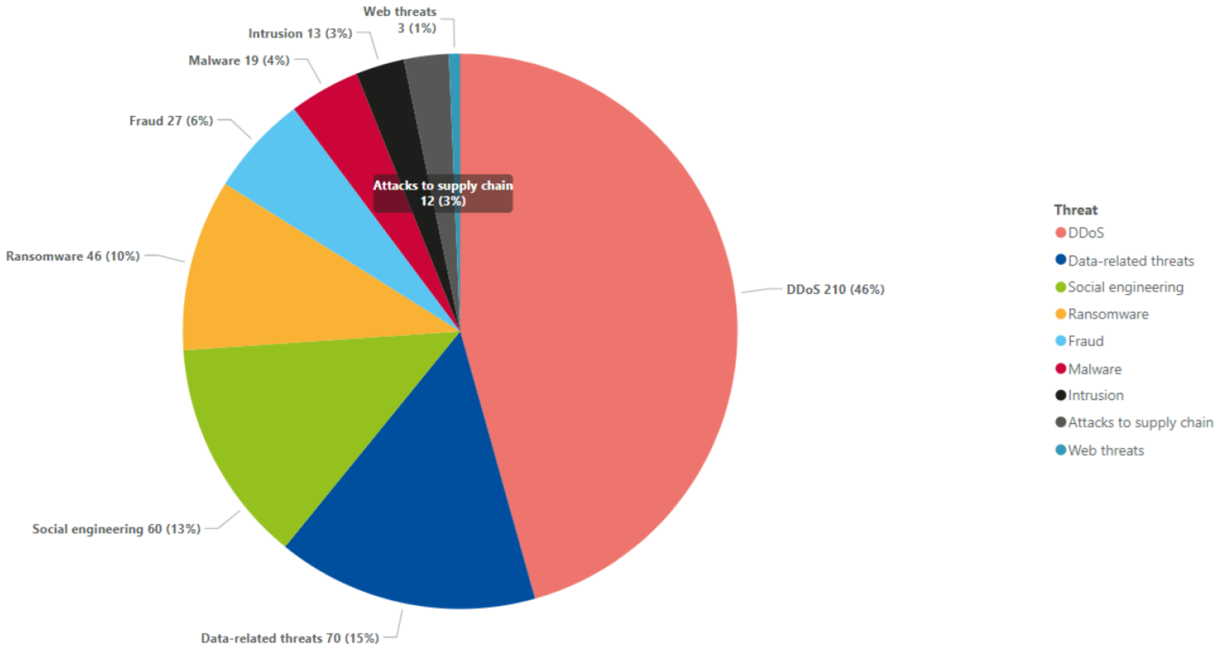


Figura 4.2: Finance-sector threat categories used as baseline for Stage 2. Source: (3).

For example, the prevalence of distributed denial-of-service reported in financial reviews, combined with availability requirements for interbank payment services, supports the creation of a PIR focused on disruption scenarios (PIR-1). Similarly, the high incidence of data-related threats and credentials theft supports a requirement focused on leakage and exposure (PIR-2), directly aligned with confidentiality obligations and the new mandates for monitoring "information of interest" on the Dark Web (9, 10, 13).

Table 4.2 presents the resulting taxonomy of ten PIRs derived from a finance-sector threat baseline and contextualized for application within the SFN.

This structured derivation is essential for traceability and auditability: each requirement is justified by sector evidence and constrained by protected scope, reducing the probability of accumulating non-essential collection topics while satisfying the Central Bank's expectation for risk-compatible monitoring.

4.6 STAGE 4: REQUESTS FOR INFORMATION FORMULATION

Stage 4 operationalizes each PIR by decomposing it into granular Requests for Information. This decomposition bridges the gap between decision-oriented requirements and what can be concretely collected, validated, and used by defensive functions. In the context of the 2025 updates, this stage is vital for fulfilling the "traceability of operations" required by Resolution BCB 538/2025 (12).

Table 4.3 illustrates the decomposition of PIR-1 into RFIs. The set covers adversarial intent, technical capability, infrastructure, and market trends, ensuring the collection plan can produce actionable outputs rather than generic situational awareness (45).

Tabela 4.2: Taxonomy of Priority Intelligence Requirements

ID	Threat Class	Lexical Triggers (examples)
PIR-1	Distributed denial-of-service	ddos; denial of service; volumetric attack; amplification; botnet
PIR-2	Data leakage and exposure	data leak; exposure; database dump; exfiltration; leaked credentials
PIR-3	Social engineering	phishing; smishing; vishing; pretexting; deepfake
PIR-4	Fraud	fraud; scam; account takeover; carding; pix fraud; unauthorized transfers
PIR-5	Ransomware	ransomware; double extortion; encryptor; RaaS; data kidnapping
PIR-6	Malware	trojan; infostealer; loader; banking trojan; mobile malware
PIR-7	Supply chain compromise	third-party; dependency; vendor compromise; PSTI; RSFN connector
PIR-8	Intrusion and post-exploitation	lateral movement; persistence; webshell; vibe hacking; RCE; privilege escalation
PIR-9	Web and mobile application threats	sql injection; xss; csrf; api security; broken authentication
PIR-10	Emerging threats	quantum; blockchain; AI agent poisoning; prompt injection; synthetic identity

4.7 STAGE 5: COLLECTION PLAN DEVELOPMENT USING 5W3H

Stage 5 consolidates the outputs of the Direction and Planning phase into a formal Collection Plan. This artifact serves as the authoritative operational reference for collection activities, specifying what will be collected, from which sources, at what frequency, and for which decision purpose. To ensure completeness and auditability, the Collection Plan is structured using the 5W3H framework (22).

In the context of the regulatory updates, this plan is no longer just a task list, but a fundamental technical control to satisfy Article 3, § 2º, inciso VI, which mandates the implementation of "traceability mechanisms" (11, 12). The 5W3H framework provides the deterministic link between the raw data collected (e.g., in the Dark Web) and the strategic PIR. By specifying the Why (linked requirement) and the How (automated filtering method), the institution creates an auditable record that must be maintained for five years according to the new Central Bank rules (12).

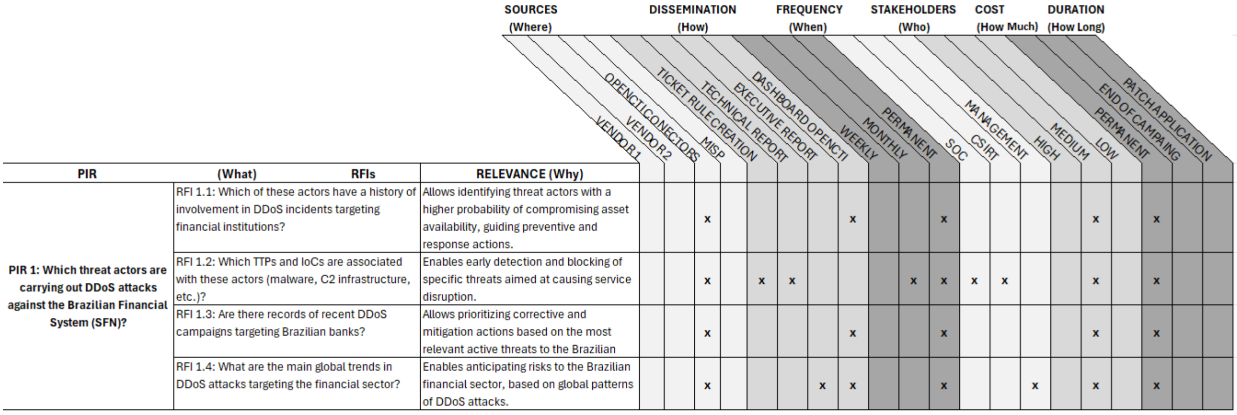
Figure 4.3 illustrates the structural logic of the 5W3H-based Collection Plan. The model visually represents how each intelligence equirement (PIR and RFI) is translated into operational parameters—such as source, frequency, method, and accountability—forming a deterministic bridge between governance-level intent and executable technical controls.

Table 4.4 presents the Collection Plan template adopted in the conceptual case study, explicitly linking operational details to intelligence requirements and risk drivers.

This level of traceability directly supports the auditability expectations of the SFN, transforming Di-

Tabela 4.3: Decomposition of PIR-1 into Requests for Information

Category	**Request for Information**	**Purpose**
RFI 1.1 (Intent and history)	Which threat groups have a documented history of targeting financial institutions in Brazil with volumetric attacks in the last 12 months?	Establishes intent and relevance.
RFI 1.2 (Capability)	What techniques (e.g., amplification protocols, botnets) are used by these actors and could bypass existing mitigation controls?	Identifies capability and defensive gaps.
RFI 1.3 (Infrastructure)	Are there active observables associated with these campaigns that can be ingested into defensive platforms?	Enables technical detection and correlation.
RFI 1.4 (Trends)	What emerging trends in "DDoS-as-a-Service" lower the barrier to entry for attacks against financial targets around the world?	Supports anticipatory planning.



			SOURCES (Where)				DISSEMINATION (How)				FREQUENCY (When)			STAKEHOLDERS (Who)			COST (How Much)			DURATION (How Long)		
PIR	**(What) RFIs**	**RELEVANCE (Why)**	VENDOR1	VENDOR2	OPENCTI CONECTORS	MISP	TICKET RULE CREATION	TECHNICAL REPORT	EXECUTIVE REPORT	DASHBOARD OPENCTI	WEEKLY	MONTHLY	PERMANENT	SOC	CSIRT	MANAGEMENT	HIGH	MEDIUM	LOW	PERMANENT	END OF CAMPAING	PATCH APPLICATION
PIR 1: Which threat actors are carrying out DDoS attacks against the Brazilian Financial System (SFN)?	RFI 1.1: Which of these actors have a history of involvement in DDoS incidents targeting financial institutions?	Allows identifying threat actors with a higher probability of compromising asset availability, guiding preventive and response actions.			x					x			x					x		x		
	RFI 1.2: Which TTPs and IoCs are associated with these actors (malware, C2 infrastructure, etc.)?	Enables early detection and blocking of specific threats aimed at causing service disruption.			x		x	x				x	x	x	x			x		x		
	RFI 1.3: Are there records of recent DDoS campaigns targeting Brazilian banks?	Allows prioritizing corrective and mitigation actions based on the most relevant active threats to the Brazilian			x					x			x					x		x		
	RFI 1.4: What are the main global trends in DDoS attacks targeting the financial sector?	Enables anticipating risks to the Brazilian financial sector, based on global patterns of DDoS attacks.			x				x	x			x			x		x		x		

Figura 4.3: Operational structure of the 5W3H-based Collection Plan. Source: Author.

rection and Planning from an informal activity into a defensible and repeatable process that meets the prescriptive expectations introduced in the most recent regulatory updates.

Tabela 4.4: Template for the CTI Collection Plan

Element (5W3H)	**Specification**	**Linked Requirement**	**Operational Detail**	**Audit Rationale**
What	Type of intelligence (IoCs, TTPs, actor profiles)	Associated PIR and RFI	Defines exact data fields and formats (STIX objects)	Ensures relevance to a validated requirement
Why	Purpose of collection	Risk or regulatory driver	Mapped to asset class and threat class	Demonstrates alignment with risk profile
Where (Source)	Collection source	RFI identifier	OSINT, Deep/Dark Web, RSFN connectors, internal telemetry	Supports source validation and provenance
When (Frequency)	Collection cadence	RFI criticality	Continuous, daily, weekly, or ad hoc	Enables review of timeliness and adequacy
Who (Stakeholders)	Producer and consumer	Decision owner	CTI team, SOC, risk management, PSTI supervisors	Clarifies accountability and information flow
How (Method)	Collection and processing method	Technical control	Automated ingestion, OpenCTI deterministic filtering	Supports reproducibility and control effectiveness
How Much (Cost)	Estimated resource impact	Budget or effort category	Analyst hours, licensing cost, infrastructure	Enables governance and prioritization decisions
How Long (Duration)	Validity period	Threat lifecycle	Temporary monitoring or persistent tracking	Supports 5-year log retention and data lifecycle

5 IMPLEMENTATION AND OPERATIONALIZATION

While Chapter 4 established the theoretical framework for structured Direction and Planning—defining the five stages from Strategic Alignment to the Collection Plan—this chapter details its translation into a functional, automated artifact. The objective is to demonstrate that high-level governance artifacts can be converted into deterministic logic that governs a Threat Intelligence Platform. This operationalization addresses the practical gap identified in the literature review by moving beyond descriptive models to executable code. Using the OpenCTI platform as the reference environment, this chapter describes the system architecture, the translation of strategic requirements into machine-readable configuration files, and the classification logic that enforces risk-centric scoping to ensure compliance and auditability.

5.1 IMPLEMENTATION PRINCIPLES AND DESIGN RATIONALE

The implementation was guided by four core principles derived directly from the methodological objectives outlined in the previous chapter:

- **Upstream Enforcement:** Direction and Planning decisions must be enforced "before" analytical processing, preventing irrelevant data from propagating downstream and consuming analyst cognitive load.
- **Determinism and Auditability:** All classification decisions must be explainable, reproducible, and traceable to an explicit intelligence requirement. This principle is critical for meeting the traceability requirements of Resolution BCB No. 85/2021 (9), allowing auditors to verify why specific data was collected and retained.
- **Configuration-Driven Governance:** Changes to intelligence scope must be possible without modifying source code, enabling institutional adaptation and formal approval workflows.
- **Platform-Native Integration:** The solution must operate within a TIP (OpenCTI), ensuring continuity with existing CTI workflows.

These principles directly reflect the governance-oriented nature of Direction and Planning phase and ensure that the technical architecture supports the regulatory expectations of the SFN.

5.2 OPERATIONAL ARCHITECTURE OVERVIEW

Figure 5.1 illustrates the logical architecture through which Direction and Planning is operationalized. The architecture is not designed as a monolithic ingestion pipeline, but as a layered scoping mechanism applied to STIX Domain Objects managed by OpenCTI.

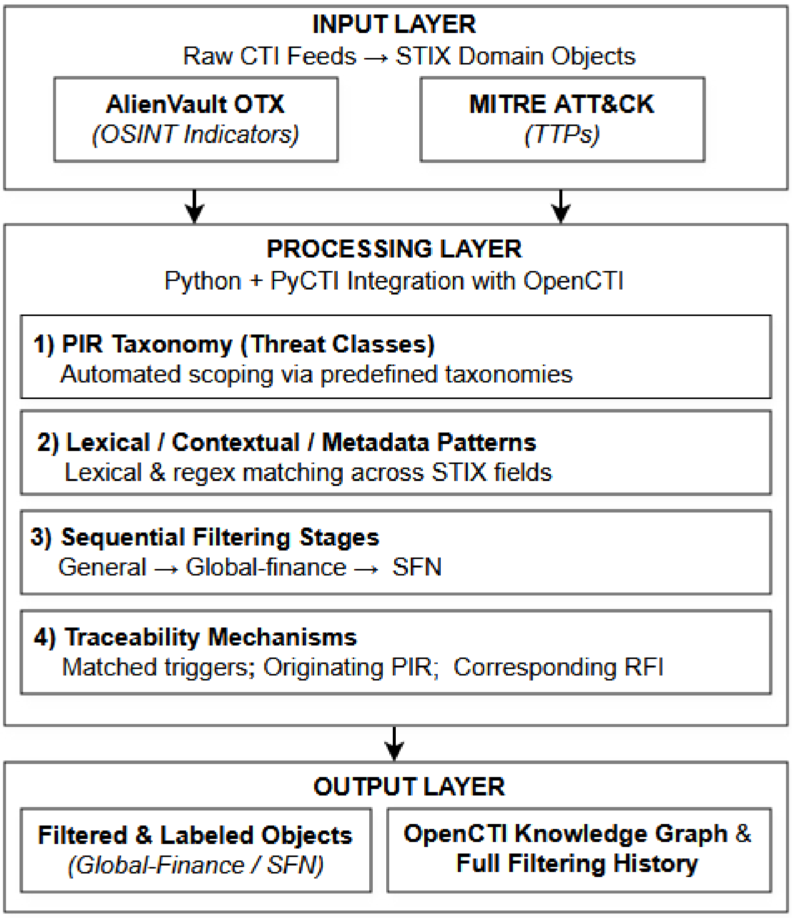

INPUT LAYER
Raw CTI Feeds → STIX Domain Objects
AlienVault OTX
(OSINT Indicators)
MITRE ATT&CK
(TTPs)
PROCESSING LAYER
Python + PyCTI Integration with OpenCTI
1) PIR Taxonomy (Threat Classes)
Automated scoping via predefined taxonomies
2) Lexical / Contextual / Metadata Patterns
Lexical & regex matching across STIX fields
3) Sequential Filtering Stages
General → Global-finance → SFN
4) Traceability Mechanisms
Matched triggers; Originating PIR; Corresponding RFI
OUTPUT LAYER
Filtered & Labeled Objects
(Global-Finance / SFN)
OpenCTI Knowledge Graph &
Full Filtering History

Figura 5.1: Operational architecture for enforcing Direction and Planning within OpenCTI.

At a high level, the architecture performs three tightly coupled activities:

1. **Retrieval:** Fetching STIX Domain Objects from the OpenCTI database.
2. **Deterministic Classification:** Applying PIR-aligned rules to label objects based on lexical and metadata patterns.
3. **Progressive Scoping:** Assigning relevance levels (General → Global-Finance → SFN) to filter noise.

Crucially, each retained object is explicitly linked to the PIR and RFI that justified its inclusion. This ensures full traceability from governance intent to technical enforcement, closing the loop between the strategic definition in Chapter 4 and the operational reality.

5.3 TECHNOLOGY STACK AND EXECUTION ENVIRONMENT

The implementation was deployed in a controlled laboratory environment designed to emulate a realistic CTI operation within the financial sector. OpenCTI was selected due to its native support for STIX 2.1, graph-based data model, and extensible API. Table 5.1 summarizes the technology stack.

Tabela 5.1: Technology stack used in the implementation

Component	Technology	Purpose
Threat Intelligence Platform	OpenCTI (v6.x)	Central CTI knowledge graph
Automation Language	Python 3.11	Rule enforcement and integration logic
API Library	pycti	Programmatic interaction with OpenCTI
Data Format	JSON	Externalized PIR and rule definitions
Containerization	Docker	Reproducible deployment

5.4 CONFIGURATION-DRIVEN DEFINITION OF PIRS

A central design decision was to externalize all Direction and Planning artifacts into structured configuration files. This acts as the machine-readable counterpart to the PIRs defined in Chapter 4 (Section 4.5). By encoding PIRs in JSON, the system allows the Collection Plan to be updated by governance teams without requiring code changes, adhering to the principle of separation between logic and policy.

Listing 5.1 presents a real excerpt from the implementation, showing how a strategic requirement (PIR-1) is translated into technical configuration.

Listing 5.1: Example of PIR definition used in the implementation

```
{
  "pir_id": "PIR-1",
  "name": "Distributed Denial-of-Service Targeting Financial Services",
  "sector": "Financial",
  "keywords": [
    "ddos",
    "denial of service",
    "volumetric attack",
    "amplification",
    "botnet"
  ]
}
```

This structure directly reflects the outputs of Stages 2 (Threat Mapping) and 3 (PIR Definition) of the methodology, allowing institutions to refine threat focus based on their risk profile, regulatory exposure, and threat landscape maturity.

5.5 PIR-BASED CLASSIFICATION AND LABELING LOGIC

The core operational mechanism of the implementation is a deterministic classification engine that evaluates STIX Domain Objects against the PIR-aligned rules defined above. This logic is implemented in the `classifier_core.py` module.

The classifier inspects selected STIX fields—such as `name`, `description`, and `external references`—and applies lexical matching to determine relevance. Listing 5.2 presents an excerpt of the classification logic.

Listing 5.2: Excerpt of PIR-based classification logic

```
def matches_pir(stix_object, pir):
    searchable_fields = [
        stix_object.get("name", ""),
        stix_object.get("description", "")
    ]

    for keyword in pir["keywords"]:
        if any(keyword.lower() in field.lower() for field in searchable_fields):
            return True
    return False
```

When a match is identified, the object is enriched with labels corresponding to the relevant PIR. This automated tagging converts the abstract "intent"of the PIR into a concrete digital artifact attached to the data, facilitating immediate filtering and retrieval by analysts.

This mechanism ensures that relevance decisions are consistently enforced at the object level, directly linking technical classification outcomes to formally defined intelligence requirements.

5.6 PROGRESSIVE SCOPING AND CONTEXTUAL LABELS

Beyond simple classification, the implementation applies progressive scoping labels that reflect increasing contextual relevance. This is the technical realization of Stage 1 (Strategic Alignment), ensuring that data is not just "financial" in nature, but specifically relevant to the Brazilian context:

- **General:** Intelligence relevant to cyber threats in general (Baseline).
- **Global-Finance:** Intelligence explicitly related to the financial sector globally.
- **SFN:** Intelligence contextualized to the Brazilian National Financial System (e.g., mentioning PIX, Brazilian banks, or local infrastructure).

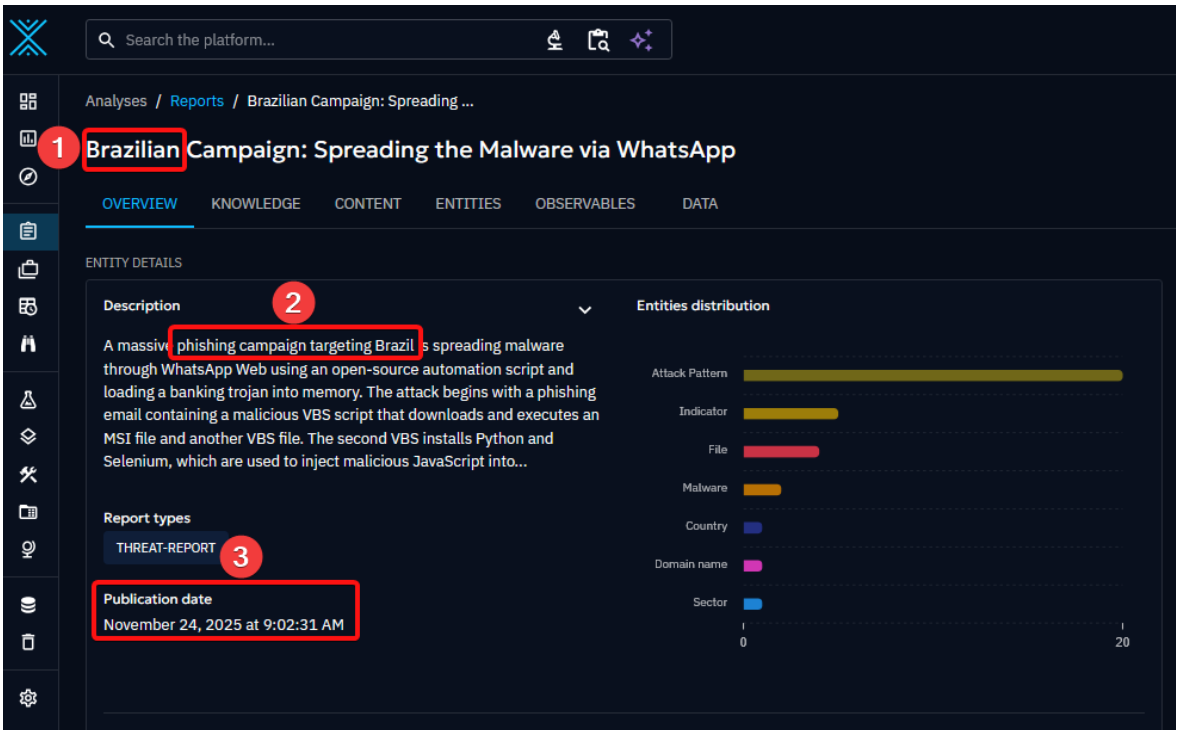
These labels are not merely descriptive; they act as technical enforcement points that constrain downstream analysis and reporting. Only objects reaching the "SFN" or "Global-Finance" scope trigger alerts or inclusion in high-priority reports. This mechanism directly enables the quantitative noise reduction presented in Chapter 6.

It is important to note that indicators and other STIX objects may exist independently of reports or campaigns within OpenCTI. The proposed methodology deliberately does not require report-level context; instead, relevance is inferred through deterministic, object-level lexical and contextual cues. Objects lacking sufficient sectoral or geographic context are retained at general scoping, reducing analyst distraction.

5.6.1 Execution Flow and Enforcement Within OpenCTI

The enforcement workflow is orchestrated by the main integration module, which periodically retrieves newly ingested STIX objects from OpenCTI, evaluates them against PIR-aligned rules, and updates the platform with both PIR labels and scoping labels. This design ensures that Direction and Planning decisions are applied consistently across ingestion cycles, rather than being left to ad hoc analyst interpretation.

Figure 5.2 illustrates an example of object-level enforcement on a threat report whose content contains lexical cues mapped to PIR-3. In this case, the keyword "phishing"—defined in table 4.2—appears directly in the report narrative, enabling deterministic classification based on the same searchable fields described in Section 5.5 (e.g., `name` and `description`). The highlighted elements show that the report is explicitly contextualized to Brazil, reinforcing the downstream assignment of institutional scope when applicable.



Search the platform...

Analyses / Reports / Brazilian Campaign: Spreading ...

Brazilian Campaign: Spreading the Malware via WhatsApp

OVERVIEW KNOWLEDGE CONTENT ENTITIES OBSERVABLES DATA

ENTITY DETAILS

Description

A massive phishing campaign targeting Brazil is spreading malware through WhatsApp Web using an open-source automation script and loading a banking trojan into memory. The attack begins with a phishing email containing a malicious VBS script that downloads and executes an MSI file and another VBS file. The second VBS installs Python and Selenium, which are used to inject malicious JavaScript into...

Report types

THREAT-REPORT

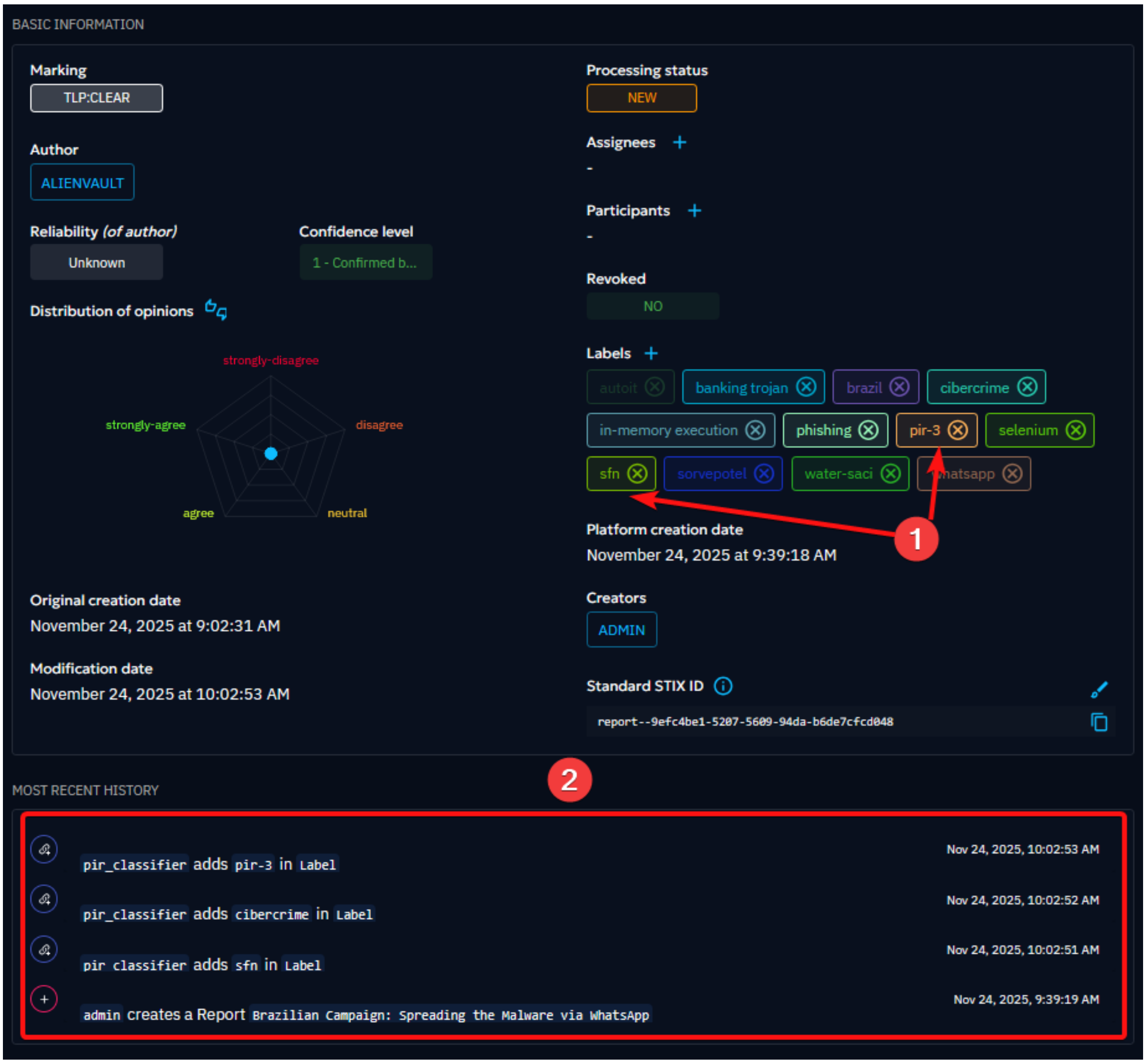
Publication date

November 24, 2025 at 9:02:31 AM

Entities distribution

Figura 5.2: Example of PIR-3 enforcement in OpenCTI.

Beyond visibility, the key governance contribution of this approach is traceability. Figure 5.3 shows that OpenCTI retains a platform-native audit trail that records (i) when the report was created in the knowledge base, and (ii) when each label was applied by the enforcement component. In the illustrated example, the object receives both the `sfn` scoping label and the `pir-3` label, and the system history provides timestamped evidence of these actions. This means that an auditor, risk manager, or reviewer can inspect a single object and determine "what" was ingested, "why" it was retained (linked PIR), "how" it relates to the institution (scope), and "when" the enforcement occurred.



BASIC INFORMATION

Marking
TLP:CLEAR

Author
ALIENVAULT

Reliability *(of author)*
Unknown

Confidence level
1 - Confirmed b...

Distribution of opinions

Original creation date
November 24, 2025 at 9:02:31 AM

Modification date
November 24, 2025 at 10:02:53 AM

Processing status
NEW

Assignees +
-

Participants +
-

Revoked
NO

Labels +
autoit ⊗ banking trojan ⊗ brazil ⊗ cibercrime ⊗
in-memory execution ⊗ phishing ⊗ pir-3 ⊗ selenium ⊗
sfn ⊗ sorvepotel ⊗ water-saci ⊗ hatsapp ⊗

Platform creation date
November 24, 2025 at 9:39:18 AM

Creators
ADMIN

Standard STIX ID ⓘ
`report--9efc4be1-5207-5609-94da-b6de7cfcd048`

MOST RECENT HISTORY

```
pir_classifier adds pir-3 in Label                                   Nov 24, 2025, 10:02:53 AM
pir_classifier adds cibercrime in Label                              Nov 24, 2025, 10:02:52 AM
pir classifier adds sfn in Label                                     Nov 24, 2025, 10:02:51 AM
admin creates a Report Brazilian Campaign: Spreading the Malware via WhatsApp   Nov 24, 2025, 9:39:19 AM
```

Figura 5.3: Traceability in OpenCTI: PIR and scope labels (e.g., `pir-3` and `sfn`) and the timestamped history of label application.

From an operational standpoint, this traceability can also be used to support notification and accountability workflows. For instance, once a report is labeled as `pir-3` and scoped as `sfn`, the platform can be configured to generate analyst notifications (or automated email summaries) containing the object link, the triggering PIR, and the enforcement timestamps—converting Direction and Planning intent into an auditable, repeatable, and actionable control embedded within the TIP.

The mechanisms described in this chapter constitute the technical foundation for the experimental evaluation presented in Chapter 6. The observed reduction from over 216,000 raw STIX Domain Objects to fewer than 1,000 scoped artifacts is a direct consequence of upstream enforcement of Direction and Planning decisions operationalized through the proposed automation. By translating PIRs into deterministic and repeatable technical controls embedded within OpenCTI, the implementation establishes a direct link between institutional risk governance and operational CTI workflows.

6 EXPERIMENTAL RESULTS AND ANALYSIS

This chapter presents the results obtained from the application of the proposed Structured Direction and Planning methodology within the OpenCTI environment. The chapter first details the objectives of the experiment, the definition of test scenarios, and the evaluation metrics selected to measure success. Subsequently, the quantitative data regarding noise reduction and the qualitative analysis of informational density are presented and discussed in light of the regulatory requirements of the SFN.

6.1 OBJECTIVE OF THE EXPERIMENT

The primary objective of this experiment is to validate the hypothesis that a structured Direction and Planning phase—operationalized through PIRs and deterministic filtering—can effectively mitigate the problem of information overload in CTI operations.

Specifically, the experiment aims to:

1. Quantify the reduction of irrelevant data (informational noise) achieved by applying upstream filtering rules compared to a standard, unrestricted ingestion process.
2. Evaluate the qualitative shift in intelligence artifacts, assessing whether the methodology promotes a transition from low-value indicators (e.g., hashes, IPs) to high-value behavioral intelligence (e.g., TTPs), aligning with the Pyramid of Pain concept (46).
3. Demonstrate the methodology's capability to produce an auditable intelligence trail aligned with risk-profile governance requirements, satisfying the prescriptive mandates for "cyber intelligence actions" established by Resolution BCB No. 538/2025 and the technical guidelines of Regulatory Instruction BCB No. 664/2025 (12, 13).

6.2 EXPERIMENTAL SCENARIOS

To isolate the impact of the proposed methodology, two distinct ingestion scenarios were established within the OpenCTI platform. This comparative approach allows for a direct assessment of the "before and after" states of the intelligence database.

6.2.1 Scenario A: Baseline

Scenario A represents the "control group". It simulates the common operational reality of many organizations where data ingestion is volume-driven rather than requirement-driven.

- **Configuration:** Standard OpenCTI connectors for AlienVault OTX and MITRE ATT&CK were enabled with default settings.

- **Scope:** No sectoral, geographic, or PIR-based filters were applied. All available data regarding indicators, malware, and threat actors were ingested without any filtering or labeling mechanisms.
- **Goal:** To establish a baseline of informational noise and data overload typical of a generic CTI program.

6.2.2 Scenario B: Structured Direction and Planning (Proposed Methodology)

Scenario B represents the "experimental group", implementing the methodology defined in Chapter 4 and the technical architecture described in Chapter 5.

- **Configuration:** The python-based integration layer was activated to intercept and evaluate STIX objects before final acceptance into the analytical workflow.
- **Scope:** The filtering logic applied the 10 PIRs defined for the SFN (e.g., DDoS, PIX fraud, Ransomware), utilizing the lexical and contextual patterns tailored to the Brazilian financial sector.
- **Goal:** To measure the efficacy of the methodology in identifying and scoping only high-fidelity intelligence relevant to the SFN risk profile.

6.3 EVALUATION METRICS

The effectiveness of the methodology is assessed using three specific metrics, chosen to cover both efficiency and quality dimensions:

1. Noise Reduction Rate (NRR): A quantitative metric measuring the percentage of data discarded as irrelevant. It is calculated as:

$$NRR = \left(\frac{V_{baseline} - V_{retained}}{V_{baseline}} \right) \times 100$$

Where $V_{baseline}$ is the volume of objects in Scenario A, and $V_{retained}$ is the volume in Scenario B. A higher NRR indicates greater efficiency in mitigating overload.

2. Informational Density by STIX Class: A qualitative metric that analyzes the composition of the retained data. It measures the ratio of behavioral objects (Attack Patterns, Intrusion Sets) versus atomic indicators (IPv4, Hashes). This metric validates alignment with the Pyramid of Pain, prioritizing enduring intelligence over ephemeral data (46).

3. Regulatory Alignment Score: A compliance-oriented metric assessing whether the retained intelligence can be traced back to a documented risk or business function. This is evaluated by verifying if every retained object in Scenario B possesses a valid “PIR Link” tag, satisfying the traceability requirements of Resolution BCB No. 538/2025 (Article 3, §2º, VI) and the log retention mandates of 5 years (12).

6.4 QUANTITATIVE RESULTS: NOISE REDUCTION

The execution of the experiment using the baseline dataset from November 2025 yielded significant quantitative differences between Scenario A and Scenario B.

6.4.1 Baseline Data Volume (Scenario A)

In Scenario A, the unrestricted ingestion resulted in a total of 216,208 SDOs. This dataset comprised a vast array of global threats, many of which had no connection to the financial sector or the Brazilian context.

6.4.2 Scoped Data Volume (Scenario B)

In Scenario B, the application of the structured Direction and Planning filters occurred in two stages:

1. **Global-Finance Filtering:** Reducing the dataset to objects relevant to the global financial sector.
2. **SFN Contextualization:** Further refining the dataset to objects containing triggers relevant to the Brazilian context (e.g., "BR", "Brazil", "PIX", "Boleto", "gov.br").

As shown in Table 6.1, the application of the structured Direction and Planning filters progressively reduced the dataset across the two stages, culminating in a Noise Reduction Rate (NRR) of 99.58%. This result empirically demonstrates the effectiveness of upstream scoping in constraining analytical workload and increasing informational density prior to downstream processing.

Tabela 6.1: Data Volume Reduction Across Filtering Stages

Filtering Stage	Object Count	Noise Reduction (NRR)	Remaining (%)
Scenario A (Baseline)	216,208	-	100.00%
Global-Finance Filter	10,007	95.37%	4.63%
Scenario B (SFN Final)	**903**	**99.58%**	**0.42%**

From an operational perspective, this level of reduction substantially narrows the analytical surface prior to downstream enrichment and correlation processes. By constraining the dataset to contextually relevant objects, the methodology shifts the analytical effort from broad ingestion toward targeted investigation, reinforcing the role of structured Direction and Planning as a control mechanism rather than a post-processing enhancement.

6.5 QUALITATIVE ANALYSIS: INFORMATIONAL DENSITY

Beyond volume reduction, the experiment evaluated the nature of the retained intelligence (Metric 2). Figure 6.1 illustrates the retention rates broken down by STIX object classes.

The analysis reveals a structural shift in the intelligence profile:

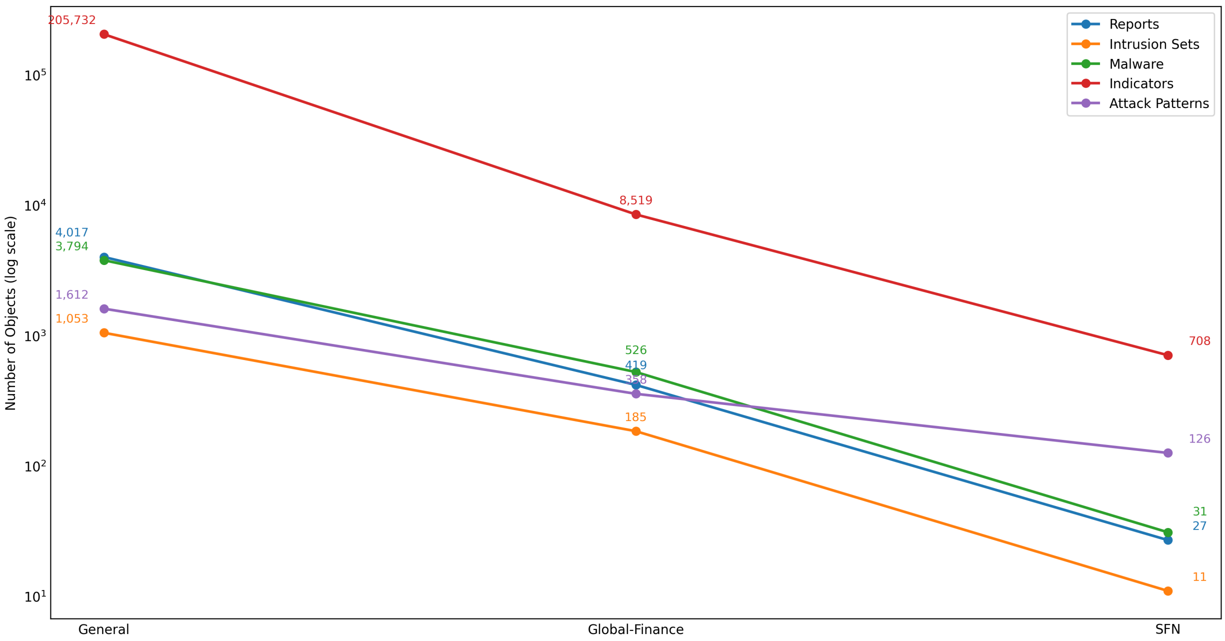


Figura 6.1: Retention rates by STIX Domain Object class after contextual filtering.

- **Atomic Indicators (0.34% Retention):** Low-level indicators such as IPs and Hashes had the lowest retention rate. This is positive, as these indicators are ephemeral and often generate false positives if not strictly scoped.
- **Attack Patterns (7.80% Retention):** Objects describing Tactics, Techniques, and Procedures had a significantly higher retention rate.

This disparity confirms that the methodology prioritizes behavioral intelligence. By retaining a higher proportion of Attack Patterns (e.g., T1078 - Valid Accounts, often used in SFN fraud scenarios) compared to simple indicators, the system aligns with the upper levels of the Pyramid of Pain. This supports a proactive defense posture, fulfilling the requirements for "intrusion detection and prevention" mandated by the 2025 regulatory update (11).

6.6 REGULATORY COMPLIANCE VALIDATION

The final metric, Regulatory Alignment, was validated through the traceability features of the implementation. In Scenario B, every retained object was automatically tagged with its originating PIR ID (e.g., PIR-1: DDoS) and its specific rationale.

This mechanism provides concrete evidence for compliance with the broader regulatory framework of the Brazilian National Financial System. Specifically, it addresses:

1. **Risk Profile Alignment (CMN and BCB):** The updated Resolution CMN No. 5.274/2025 and Resolution BCB No. 538/2025 mandate 14 specific procedures and controls (11, 12). By demonstrating that 99.58% of noise was rejected and that 100% of retained data is linked to a strategic requirement,

the methodology proves that intelligence activities are strictly driven by the institution's specific risk appetite, fulfilling the "compatibility with risk profile" mandate (Art. 2).

2. **Auditability and Traceability Mechanisms:** These resolutions now explicitly require "traceability mechanisms" (Art. 3, §2º, VI) and the maintenance of action plans for 5 years (12). The proposed method transforms CTI from a subjective activity into an auditable process, where every ingested artifact can be traced back to a documented business requirement and documented within the OpenCTI history.

3. **Mandatory Cyber Intelligence Actions:** Furthermore, the approach directly satisfies the requirements for "cyber intelligence actions" established by Resolutions CMN No. 5.274/2025 and BCB No. 538/2025 (11, 12), and detailed by Normative Instruction BCB No. 664/2025 (13). These regulations mandate the monitoring of "information of interest" (clients, keys, credentials, vulnerabilities) across the surface web, Deep Web, Dark Web, and private communication groups. The methodology provides the technical roadmap to execute these mandatory monitoring actions without incurring informational overload.

7 DISCUSSION: OPERATIONAL, STRATEGIC, AND REGULATORY IMPLICATIONS

The quantitative results presented in Chapter 6 demonstrate a noise reduction of approximately 99.58% and a significant increase in the retention of behavioral intelligence (Attack Patterns). While these metrics validate the technical efficacy of the proposed methodology, the broader contribution of this research lies in how these results translate into Operational efficiency, Strategic resilience, and Regulatory compliance within the SFN. This chapter interprets these findings, positioning the methodology not merely as a filtering mechanism, but as a governance instrument that addresses the structural gaps identified in the literature review.

7.1 OPERATIONAL IMPLICATIONS: FROM REACTIVE TRIAGE TO PROACTIVE SCOPING

The most immediate operational implication of the proposed methodology is the shift from a “downstream scoring” paradigm to an “upstream scoping” paradigm. As discussed in Chapter 3, approaches such as the "Enriched Threat Intelligence Platform" by Faiella et al. (30) rely on ingesting vast amounts of data to subsequently score and prioritize alerts. While valid, this approach imposes a heavy computational and cognitive burden on the SOC, which must process noise before identifying signal.

In contrast, by operationalizing PIRs as deterministic pre-ingestion filters, the proposed methodology prevented 216,208 irrelevant objects from entering the analytical pipeline. This has two profound operational consequences:

1. **Reduction of Cognitive Load:** By eliminating 99.58% of generic data upstream, analysts are liberated from the fatigue of triaging low-fidelity indicators. This directly addresses the “information overload” challenge identified by Tounsi and Rais (7) as a primary cause of CTI inefficiency.
2. **Ascension in the Pyramid of Pain:** The qualitative analysis in Chapter 6 revealed a high retention rate of Attack Patterns (7.80%) compared to atomic Indicators (0.34%). This confirms that a PIR-driven approach naturally filters out ephemeral observables (hashes, IPs) while preserving enduring knowledge about adversary behaviors (TTPs). Operationally, this empowers defensive teams to focus on detecting "how" adversaries operate (Operational/Tactical CTI) rather than chasing "what" infrastructure they used in the past, fostering a more proactive defense posture.

7.2 STRATEGIC IMPLICATIONS: DEMOCRATIZATION AND CONTINUOUS RESILIENCE

From a strategic perspective, the methodology offers a pathway to democratize mature CTI capabilities across the financial sector, particularly for institutions with limited resources.

7.2.1 Enabling Small and Medium CTI Teams

In the Brazilian SFN, institutions classified as Segment 3 (S3) and Segment 4 (S4) face regulatory requirements comparable to those of large banks (47) but often operate with constrained cybersecurity budgets and smaller teams. The experimental results suggest that structured Direction and Planning acts as a force multiplier. By automating the relevance filtering process, the methodology reduces the dependency on large-scale big data analytics platforms and specialized triage teams. This makes it feasible for smaller institutions to maintain a CTI program that is both effective and compliant, without the prohibitive costs associated with unstructured data ingestion and analysis.

7.2.2 Continuous Monitoring versus Episodic Validation

Established frameworks such as TIBER-EU (36) and CBEST (37) represent the gold standard for intelligence-led resilience validation. However, as noted in the literature review, these frameworks are inherently episodic—designed for periodic red teaming exercises. The methodology proposed in this dissertation fills the gap between these exercises. It converts the threat scenarios typically defined in TIBER/C-BEST into continuous monitoring rules. By doing so, it ensures that the institution maintains situational awareness of its priority threats on a daily basis, rather than only during annual or triennial validation tests.

7.3 REGULATORY IMPLICATIONS: TRACEABILITY AND AUDITABILITY

The Brazilian regulatory framework for cybersecurity (Resolution CMN No. 4.893/2021 (10) and Resolution BCB No. 85/2021 (9)) is explicitly risk-based. It requires that cybersecurity policies be compatible with the institution's risk profile and that controls be traceable.

The proposed methodology provides a concrete mechanism to satisfy these abstract regulatory mandates:

- **Proof of Alignment (Risk Profile):** By deriving PIRs directly from critical asset classes (Stage 1) and sector-specific threat mapping (Stage 2), the methodology ensures—and documents—that data collection is driven by the institution's specific risk profile, not by generic feeds.
- **Auditability of Intelligence:** The use of the 5W3H framework in the Collection Plan (Stage 5) creates an unbreakable audit trail. Every intelligence object retained in the platform can be traced back to a specific RFI, which links to a PIR, which ultimately links to a business risk. This allows

an institution to demonstrate to regulators exactly "why" resources are being allocated to monitor specific threats, satisfying the governance requirements for accountability.

7.4 PRACTICAL LIMITATIONS AND OPERATIONAL CONSIDERATIONS

Despite the demonstrated efficacy in noise reduction and regulatory alignment, the proposed methodology presents inherent limitations that must be acknowledged to ensure realistic operational expectations.

7.4.1 Dependency on Lexical and Taxonomy Maintenance

The core filtering mechanism relies on deterministic rules based on lexical triggers (keywords, tags, regex) derived from the PIRs. While efficient, this approach is brittle against terminology shifts. As noted by Tounsi and Rais (7), the cyber threat landscape is highly dynamic; threat actors frequently rebrand, and new malware families emerge with names that may not match existing filters. Consequently, the methodology requires a continuous maintenance cycle for the Threat Mapping (Stage 2) and PIR definitions (Stage 3). If the taxonomy is not updated to reflect new threat nomenclatures (e.g., a new ransomware strain named “DarkSide” appearing when the filter only looks for “WannaCry”), the system will produce false negatives, filtering out relevant intelligence.

7.4.2 The Ephemerality of Technical Indicators

The methodology focuses on filtering incoming STIX objects, many of which are atomic indicators (IPs, hashes). Research by Silva et al. (14) and Tounsi and Rais (7) highlights that such indicators have a very short operational lifespan. Even with effective filtering, there is a risk that by the time an indicator is ingested, processed, and matched to a PIR, it may already be obsolete. While this methodology increases the "relevance" of the indicators retained, it does not inherently solve the problem of their "timeliness" or utility if the adversary has already rotated their infrastructure.

7.4.3 Limitations of Open Source Intelligence

The experimental validation relied primarily on OSINT feeds (AlienVault OTX, MITRE ATT&CK). While sufficient for a conceptual case study, OSINT sources often suffer from higher rates of false positives and lack the context found in premium, curated intelligence feeds. In a production environment within the SFN, reliance solely on the sources used in this experiment would likely result in gaps regarding deep-web threats or financial fraud specifics that are typically gated behind commercial vendors or closed trust groups (e.g., FS-ISAC, Axur, IronFence, Apura) (48, 49, 50, 51). Therefore, the 99.58% reduction rate should be viewed as a baseline for open sources; curated feeds might exhibit different noise-to-signal ratios.

7.4.4 Deterministic versus Probabilistic Reasoning

Finally, unlike advanced models using Graph Neural Networks (EGNN) as proposed by Zhang et al. (38), the proposed methodology uses deterministic logic. It does not infer hidden relationships or predict links that are not explicitly defined in the data. While this ensures the high auditability required by SFN regulations, it limits the system's ability to detect "unknown unknowns" or subtle semantic connections that probabilistic AI models might identify. Thus, this methodology should be viewed as a foundational governance layer, potentially to be augmented by advanced analytics as the organization's CTI maturity grows.

8 CONCLUSION AND FUTURE WORK

The exponential growth of cyber threats targeting Critical Infrastructures has intensified a structural challenge within CTI operations: information overload. As identified in the literature review, the proliferation of heterogeneous threat data frequently overwhelms analysts and dilutes decision-making effectiveness. This phenomenon is exacerbated when collection activities are not guided by explicit strategic intent, leading to a reactive posture where defenders consume resources filtering noise rather than analyzing threats. In the Brazilian context, the promulgation of the prescriptive 2025 regulatory framework has transformed CTI from a recommended capability into a mandatory, auditable technical control, raising the stakes for methodological rigor (11, 12).

This dissertation addressed this challenge by proposing, implementing, and validating a structured methodology for the Direction and Planning phase of the intelligence cycle. Specifically tailored to the regulatory and operational context of the SFN, the research challenged the prevailing paradigm that seeks to improve intelligence quality solely through post-collection enrichment. Instead, this work demonstrated that upstream scoping—anchored in institutional risk, new regulatory mandates for Dark Web monitoring, and PIRs—constitutes a more efficient, governable, and resilient approach to managing Cyber Threat Intelligence (13).

8.1 SYNTHESIS OF CONTRIBUTIONS AND OBJECTIVES

This research was guided by the general objective of developing and validating a structured methodology for the DP phase aimed at reducing informational noise and aligning intelligence production with the SFN's requirements. This objective was successfully achieved through the definition of the five-stage framework (Chapter 4), its technical implementation in OpenCTI (Chapter 5), and its validation through a case study (Chapter 6).

Specifically, the research met its specific objectives as follows:

1. **Define a Taxonomy of Intelligence Requirements:** Addressed in Chapter 4 (Stage 3). The research established a structured framework for Priority Intelligence Requirements grounded in an asset-centric and risk-centric perspective. By mapping critical financial assets to verified threat landscapes, a taxonomy of 10 SFN-specific PIRs was created, translating abstract risks into concrete intelligence directives.

2. **Operationalize the 5W3H Method:** Addressed in Chapter 4 (Stage 5). The classical 5W3H framework was adapted to structure the CTI Collection Plan. This ensured that every collection task had defined attributes for source (Where), justification (Why), and consumer (Who), transforming the collection plan into an auditable governance artifact that satisfies the "traceability of operations" required by Resolution BCB 538/2025 (12).

3. **Automate Threat Data Filtering:** Addressed in Chapter 5. The proposed methodology was translated into executable python code integrated with the OpenCTI platform. This implementation successfully converted the theoretical PIRs into deterministic lexical and contextual rules, enabling the automated scoping of intelligence artifacts before they enter the analytical workflow.

4. **Support Regulatory Compliance:** Addressed throughout Chapters 4 and 6. The methodology directly supports compliance with Resolutions CMN 5.274/2025 and BCB 538/2025 by ensuring that data collection is compatible with the institution's risk profile and includes mandatory monitoring of the Deep and Dark Web (13). The traceability provided by the PIR-to-Object linking mechanism offers the proof of control required the SFN regulatory framework.

5. **Validate Methodological Effectiveness:** Addressed in Chapter 6. The quantitative efficacy was validated through a conceptual case study. The application of the methodology reduced a baseline dataset of 216,208 raw objects to 903 relevant artifacts, achieving a 99.58% noise reduction. This result is particularly significant given the expanded collection mandates of 2025 regulatory updates, proving that upstream scoping is the only viable path to manage the volume of "information of interest" required by the Central Bank.

8.2 FUTURE WORK

While the results achieved in this dissertation are significant, the limitations discussed in Chapter 7 highlight several avenues for future research and practical evolution of the proposed methodology.

8.2.1 Operational Deployment and PSTI Risk Monitoring

Future work should focus on transitioning from the conceptual case study to deploying the proposed pipeline within a live financial institution. A critical area for expansion is the monitoring of Information Technology Service Providers (PSTIs). Following the C&M Software (CMSW) incident in 2025, where supply chain compromise led to systemic fraud, future iterations of the methodology should include specific PIRs for third-party infrastructure and credential exposure (27).

Beyond measuring noise reduction, future studies should assess operational metrics such as *Mean Time to Triage* (MTTT) and the practical effectiveness of intelligence workflows in preventing third-party enabled attacks and other forms of credential abuse. Additionally, incorporating data quality metrics—such as false positives, false negatives, precision, and recall—will provide a more granular evaluation of the methodology's performance, enabling continuous improvement and alignment with real-world threat dynamics.

8.2.2 Integration with Natural Language Processing (NLP) and LLMs

As noted in the limitations, the reliance on lexical and regex-based filtering constitutes a constraint regarding semantic flexibility. Future iterations of the methodology should explore the integration of Natural

Language Processing techniques and Large Language Models (LLMs) to semantically evaluate incoming intelligence against PIRs, especially to identify AI-driven threats like "vibe hacking" that may use novel terminology (40). This hybrid approach—combining deterministic filtering for auditability with probabilistic NLP for adaptability—represents the next frontier for intelligent scoping.

8.2.3 Cross-Sector Adaptability and Critical Infrastructure Interdependence

The National Strategy for Critical Infrastructure Security emphasizes the interdependence between sectors such as finance, energy, telecommunications, and transportation. Future research should adapt the proposed Direction and Planning framework to these other critical sectors. By recalibrating Stage 1 (Strategic Alignment) and Stage 2 (Threat Mapping) to reflect the specific assets and threats of the energy or telecom sectors (e.g., SCADA systems, 5G infrastructure), the methodology could be generalized, strengthening national-level cyber resilience.

8.2.4 Harmonization with Mandatory Threat-Led Testing

Finally, further research should investigate how continuous, PIR-driven monitoring can be systematically integrated with the annual intrusion tests now mandated by Resolution BCB 538/2025 (12). Developing mechanisms to promote high-priority threat patterns identified through continuous CTI operations into Red Team targeting scenarios represents a promising direction. This would create a unified feedback loop where daily intelligence informs mandatory annual testing, ensuring that security assessments are grounded in the actual threat landscape facing the SFN.

In conclusion, this dissertation demonstrates that structured Direction and Planning is not merely a preparatory step in the intelligence cycle, but a strategic and technical control mechanism capable of transforming Cyber Threat Intelligence into a risk-aligned, auditable, and decision-oriented capability. By anchoring intelligence collection in institutional priorities and in the recently updated prescriptive regulatory mandates governing the financial sector, the proposed methodology offers a sustainable path for managing cyber threat complexity within the Brazilian National Financial System and beyond.

REFERENCES

1 CREST. *Cyber Threat Intelligence*. [S.l.], 2022. Acessed: 2026-02-24. Disponível em: <https://www.crest-approved.org/wp-content/uploads/2022/04/CREST-Cyber-Threat-Intelligence.pdf>.

2 UK Ministry of Defence. *Joint Doctrine Publication 2-00: Intelligence, Counter-intelligence and Security Support to Joint Operations*. [S.l.], 2023. Acessed: 2026-02-24. Disponível em: <https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf>.

3 ENISA. *Threat Landscape: Finance Sector*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf>.

4 Presidência da República. *Decreto nº 9.573, de 22 de novembro de 2018: Política Nacional de Segurança de Infraestruturas Críticas*. 2018. Acessed: 2026-02-24. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Decreto/D9573.htm>.

5 Presidência da República. *Decreto nº 11.856, de 26 de dezembro de 2023: Política Nacional de Cibersegurança*. 2023. Acessed: 2026-02-24. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm>.

6 Banco Central do Brasil. *Sistema Financeiro Nacional*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/sfn>.

7 TOUNSI, W.; RAIS, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, v. 72, p. 212–233, 2018. Disponível em: <https://doi.org/10.1016/j.cose.2017.09.001>.

8 Presidência da República. *Decreto nº 10.569, de 9 de dezembro de 2020: Estratégia Nacional de Segurança de Infraestruturas Críticas*. 2020. Acessed: 2026-02-24. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Decreto/D10569.htm>.

9 Banco Central do Brasil. *Resolução BCB nº 85, de 8 de abril de 2021*. 2021. Acessed: 2026-02-24. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=85&tipo=Resolu%C3%A7%C3%A3o+BCB>.

10 Conselho Monetário Nacional. *Resolução CMN nº 4.893, de 26 de fevereiro de 2021*. 2021. Acessed: 2026-02-24. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=4893&tipo=Resolu%C3%A7%C3%A3o+CMN>.

11 Conselho Monetário Nacional. *Resolução CMN nº 5.274, de 18 de dezembro de 2025. Altera a Resolução CMN nº 4.893/2021*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5274>.

12 Banco Central do Brasil. *Resolução BCB nº 538, de 18 de dezembro de 2025. Altera a Resolução BCB nº 85/2021*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=538>.

13 Banco Central do Brasil. *Instrução Normativa BCB nº 664, de 11 de setembro de 2025. Estabelece prazos e requisitos para ações de inteligência cibernética*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=664>.

14 SILVA, R. de O.; ALBUQUERQUE, R. de O.; GONDIM, J. J. C. Methodology to improve the quality of cyber threat intelligence production through open source platforms. In: *International Conference on Computer Science, Electronics and Industrial Engineering (CSEI)*. [s.n.], 2023. p. 86–98. Disponível em: <https://doi.org/10.1007/978-3-031-30592-4_7>.

15 Department of Defense. *Joint Publication 2-0: Joint Intelligence*. [S.l.], 2013. Acessed: 2026-02-24. Disponível em: <https://www.benning.army.mil/infantry/doctrinesupplement/atp3-21.8/PDFs/jp2_0.pdf>.

16 NATO. *Allied Joint Doctrine for Intelligence Procedures (AJP-2.1)*. 2016.

17 Joint Chiefs of Staff. *Joint Doctrine for Intelligence Support to Operations*. [S.l.], 1995. Acessed: 2026-02-24. Disponível em: <https://apps.dtic.mil/sti/tr/pdf/ADA327792.pdf>.

18 U.S. Marine Corps. *MCWP 2-2: MAGTF Intelligence Collection*. [S.l.], 2004. Acessed: 2026-02-24. Disponível em: <https://www.marines.mil/Portals/1/Publications/MCWP%202-2%20MAGTF%20Intelligence%20Collection.pdf>.

19 United States Department of the Army. *Collection Management and Synchronization Planning*. Washington, DC, 1994. Acessed: 2026-02-24. Disponível em: <https://irp.fas.org/doddir/army/fm34-2/Appd.htm>.

20 LOPEZ, E. M.; AWAD, A. I. *A Framework to Establish a Threat Intelligence Program*. Dissertação (Mestrado) — Luleå University of Technology, 2021. Acessed: 2026-02-24. Disponível em: <https://research.uaeu.ac.ae/en/publications/a-framework-to-establish-athreat-intelligence-program/>.

21 DEBOLT, M.; CONNOR, C. et al. *Cyber Threat Intelligence Capability Maturity Model (CTI-CMM), Version 1.2*. [S.l.], 2024. Acessed: 2026-02-24. Disponível em: <https://img1.wsimg.com/blobby/go/9aad51ed-ae49-4d8d-ba52-3af7e504ddf1/downloads/2accb54e-ec3a-49e4-bfa4-1d7abbafbe8a/CTI-CMM%20book%20Version%201.2%20web%20amended.pdf?ver=1757523856600>.

22 SLOAN, M. C. Aristotle's as the original locus for the septem circumstantiae. *Classical Philology*, v. 105, n. 3, p. 236–251, 2010. Disponível em: <https://doi.org/10.1086/656196>.

23 Central Bank of Brazil. *Pix at 5 — The innovation that transformed payments in Brazil*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.bcb.gov.br/en/pressdetail/2640/nota>.

24 Banco Central do Brasil. *Pix bate novo recorde diário de transações*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/pix-em-numeros-estatisticas>.

25 IBM Security. *Cost of a Data Breach Report 2025 — Brazil Highlights*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.ibm.com/downloads/documents/br-pt/131cf87b20b31c91>.

26 Federação Brasileira de Bancos (Febraban). *Pesquisa Febraban de Tecnologia Bancária 2025*. 2025. Acessed: 2026-02-24. Disponível em: <https://portal.febraban.org.br/noticia/4278/pt-br/>.

27 MARTÍNEZ, G. The perfect storm: The largest cyberattack on brazil's financial system (c&m software incident). *LACNIC CSIRT / Bttng Apura Report*, September 2025. Acessed: 2026-02-24. Disponível em: <https://blog.lacnic.net/en/the-perfect-storm-the-largest-cyberattack-on-brazils-financial-system/>.

28 OSLIAK, O.; SARACINO, A.; MARTINELLI, F.; MORI, P. Cyber threat intelligence for critical infrastructure security. *Concurrency and Computation: Practice and Experience*, v. 35, n. 7759, 2023. Disponível em: <https://doi.org/10.1002/cpe.7759>.

29 LESZCZYNA, R.; WRÓBEL, M. R. Threat intelligence platform for the energy sector. *Softw. Pract. Exp.*, v. 49, n. 8, p. 1225–1254, 2019. Disponível em: <https://doi.org/10.1002/spe.2705>.

30 FAIELLA, M.; GRANADILLO, G. G.; MEDEIROS, I.; AZEVEDO, R.; ZARZOSA, S. G. Enriching threat intelligence platforms capabilities. In: *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE)*. [s.n.], 2019. p. 37–48. Disponível em: <https://doi.org/10.5220/0007830400370048>.

31 SILVA, A. de Melo e; ALBUQUERQUE, R. de O.; GONDIM, J. J. C.; VILLALBA, L. J. G. A methodology to evaluate standards and platforms within cyber threat intelligence. *Future Internet*, v. 12, n. 6, p. 108, 2020. Disponível em: <https://doi.org/10.3390/fi12060108>.

32 OASIS Cyber Threat Intelligence Technical Committee. *STIX Version 2.1. Part 1: Overview*. [S.l.], 2021. Acessed: 2026-02-24. Disponível em: <https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html>.

33 OASIS Cyber Threat Intelligence Technical Committee. *TAXII Version 2.1*. [S.l.], 2021. Acessed: 2026-02-24. Disponível em: <https://docs.oasis-open.org/cti/taxii/v2.1/taxii-v2.1.html>.

34 CISA. *Critical Infrastructure Sectors*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>.

35 Presidência da República. *Plano Nacional de Segurança de Infraestruturas Críticas*. 2022. Acessed: 2026-02-24. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm>.

36 European Central Bank. *Adopting TIBER-EU will help fulfil DORA requirements*. 2024. Acessed: 2026-02-24. Disponível em: <https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.miptopical240926.en.pdf>.

37 Bank of England. *CBEST Threat Intelligence-Led Assessments*. 2014. Acessed: 2026-02-24. Disponível em: <https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide>.

38 ZHANG, Y.; CHEN, J.; CHENG, Z.; SHEN, X.; QIN, J.; HAN, Y.; LU, Y. Edge propagation for link prediction in requirement-cyber threat intelligence knowledge graph. *Information Sciences*, v. 653, p. 119770, 2024. Disponível em: <https://doi.org/10.1016/j.ins.2023.119770>.

39 MOURATIDIS, H.; ISLAM, S.; SANTOS-OLMO, A.; SÁNCHEZ, L. E.; ISMAIL, U. M. Modelling language for cyber security incident handling for critical infrastructures. *Computers & Security*, v. 128, p. 103139, 2023. Disponível em: <https://doi.org/10.1016/j.cose.2023.103139>.

40 ANTHROPIC. *Vibe Hacking: How Cybercriminals are Using AI Coding Agents to Scale Data Extortion Operations*. [S.l.], 2025. Acessed: 2026-02-24. Disponível em: <https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf>.

41 FS-ISAC. *Navigating Cyber 2025: Annual Threat Review and Predictions*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.fsisac.com/navigatingcyber2025>.

42 Board of Governors of the Federal Reserve System. *Cybersecurity and Financial System Resilience Report*. 2024. Acessed: 2026-02-24. Disponível em: <https://www.federalreserve.gov/publications/files/cybersecurity-report-202407.pdf>.

43 Office of the Comptroller of the Currency. *Cybersecurity and Financial System Resilience Report*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.occ.gov/publications-and-resources/publications/cybersecurity-and-financial-system-resilience/files/pub-2025-cybersecurity-report.pdf>.

44 NFCERT. *Cyber Threat Landscape for the Nordic Financial Sector*. 2025. Acessed: 2026-02-24. Disponível em: <https://communication.nfcert.org/hubfs/CTL_Reports/2025%20TLP_CLEAR%20NFCERT%20Cyber%20Threat%20Landscape%20%28CTL%29%20Report%20v1.0.pdf>.

45 UK Government. *Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts*. 2019. Acessed: 2026-02-24. Disponível em: <https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf>.

46 BIANCO, D. J. *The Pyramid of Pain*. 2013. Acessed: 2026-02-24. Disponível em: <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>.

47 Conselho Monetário Nacional. *Resolução CMN nº 4.553, de 30 de janeiro de 2017*. 2017. Estabelece a segmentação prudencial das instituições financeiras. Disponível em: <https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50335/Res_4553_v2_L.pdf>.

48 FS-ISAC. *Financial Services Information Sharing and Analysis Center*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.fsisac.com/>.

49 Axur. *Axur Cyber Threat Intelligence*. 2025. Acessed: 2026-02-24. Disponível em: <https://www.axur.com>.

50 IronFence. *IronFence Cyber Threat Intelligence*. 2025. Acessed: 2026-02-24. Disponível em: <https://ironfence.ai>.

51 Apura. *Apura Cyber Threat Intelligence*. 2025. Acessed: 2026-02-24. Disponível em: <https://apura.com.br/>.